

NETERIUM

the next generation of screening infrastructure

ISO 20022 Migration and Compliance Implications

Richer Data, Smarter Compliance, Safer payments

December 2025



Executive Summary

The global migration to ISO 20022 is reshaping the payments landscape, with SWIFT mandating the use of ISO 20022 messages for cross border payments since the end of November 2025 and a significant number of national payment systems, including major economies, already live. This shift unlocks richer, standardised end-to-end payment data that can transform how institutions manage financial crime risk.

For compliance teams, ISO 20022 is both an opportunity and a forcing function. On the one hand, it delivers more and better structured data that can significantly improve sanctions screening and AML monitoring, reduce false positives, and enable more meaningful analytics and reporting. On the other hand, it introduces new complexity around data handling, screening logic, alphabet support, and system design.

Financial institutions that succeed with ISO 20022 will:

- Build screening capabilities that fully exploit the richer dataset, including structured fields, contextual information, and non-Latin scripts
- Treat compliance data as a strategic asset, using the additional context to enhance risk-based scoring, analytics, and regulatory reporting
- Move to modular, composable architectures where screening and enrichment components can be upgraded independently of case management and other downstream systems
- Design for flexibility so that new fields, identifiers, and regulatory expectations can be absorbed without repeated reformatting.

ISO 20022 is not just a technical migration. It is an opportunity to modernise compliance, strengthen risk controls, and deliver safer, more transparent financial services.

Introduction

The global migration to ISO 20022 represents one of the most significant transformations in the payments industry in decades. Since end November 2025, all SWIFT-connected institutions are required to adopt the new messaging standard, while a large number of national payment systems supporting cross-border payments – including major infrastructures such as TARGET2 (EU), CHAPS (UK), Fedwire (US), and CIPS (CN) – have already transitioned or are in the process of doing so. The move promises richer, standardized, and end-to-end payment data, enabling greater efficiency, transparency, and interoperability across the financial ecosystem.

From a compliance perspective, ISO 20022 directly addresses long-standing calls from regulators and the Financial Action Task Force (FATF) for more consistent and structured information in payment messages. The standard provides unprecedented opportunities to improve screening accuracy by leveraging additional and better structured data points. Importantly, ISO 20022 is a flexible syntax, meaning additional data elements can be introduced over time. For example, FATF guidance has highlighted the potential to include originator and beneficiary information beyond traditional fields to enhance anti-money laundering (AML) monitoring, calling for future-proof and adaptable compliance solutions.

This paper explores the implication of ISO 20022 adoption for compliance screening, and practical steps financial organisations must take to maximize benefits while managing associated risks.

ISO 20022 Migration on the SWIFT Network

The migration to ISO 20022 for payment transactions on the SWIFT network has been completed. Since the end of November 2025, all SWIFT-connected institutions must have replaced legacy MT payment messages with their ISO 20022 equivalents. While the migration began in March 2023 under a coexistence model—allowing both MT and ISO 20022 payment messages—the coexistence period ended in November 2025, after which only ISO 20022 are supported for inter-participant messaging.

This effort has been part of a broader global shift. Many of the world's national payment systems, including those of the largest economies, have already adopted ISO 20022. This ensures that richer, better-structured payment data can now flow end-to-end without truncation, enabling both the industry and its customers to fully realize the benefits of the standard.

From a compliance perspective, the transition responds directly to calls from the Financial Action Task Force (FATF), which has consistently advocated for richer, standardized data formats to improve transparency and financial crime prevention. The ISO 20022 standard itself indeed brings significant improvements over SWIFT MT messages, thereby helping to achieve better compliance.

Compliance Screening: Opportunities and Challenges

The richer and more structured ISO 20022 standard offers a substantial opportunity to strengthen compliance screening. By providing access to more granular and standardized information, it enables financial institutions to conduct more accurate and efficient checks. At the same time, it introduces new challenges and requirements for screening tools:

- **Leveraging additional data points:** ISO 20022 allows structured fields such as country, city¹, and other identifiers to complement personal names, enabling more precise scoring of alerts and reducing false positives. Screening systems must interpret these data points both semantically—for example, geolocation matching requires a different approach than the fuzzy matching of names—and contextually rather than in isolation. For instance, should “John Doe, New Jersey” in a payment message be considered a match for “John Doe, New York” in a watchlist, and how should such a compounded match be scored?
- **Supporting optional versus mandatory fields:** ISO 20022 supports additional optional fields such as date of birth of which the addition (for natural persons) is recommended by the FATF and mandatory in some jurisdictions, further adding data points when as part of the compound screening can further enhance accuracy but also add complexity to the screening logic and algorithm calibration.
- **Screening both structured and unstructured data:** While ISO 20022 introduces more structured fields, free-text elements (such as ‘purpose’ or ‘remittance information’) remain part of the messages and must still be screened. Compliance systems must therefore be capable of effectively handling both unstructured text and structured data elements to ensure comprehensive screening.

¹ From November 2025, a “hybrid address” format—where country and city must be captured in dedicated fields -while other elements can remain in free text—will be introduced alongside the fully structured address format. The fully unstructured format (100% free text) will be decommissioned in November 2026, leaving only hybrid and fully structured options. This evolution will further enhance compliance outcomes by enabling more accurate and reliable screening of address data.

- **Multi-alphabet support:** Unlike legacy MT messages, ISO 20022 supports the use of non-Latin characters. As watchlist data providers increasingly include names and aliases in their native alphabets, the ability to screen using these original scripts—rather than relying solely on transliterated versions—significantly enhances screening accuracy. Screening solutions must therefore be capable of handling multiple writing systems to ensure complete and reliable coverage
- **Provide contextual insights:** ISO 20022 provides the structured and contextual information required for a far more comprehensive analysis of transactions compared to legacy MT messages. By capturing all parties in the payment chain—including the ultimate debtor and ultimate creditor—along with contextual elements such as payment purpose and remittance information, it enables a much deeper understanding of each transaction. This richer context allows for more sophisticated screening: for instance, by analysing the complete transaction details, it becomes possible to identify multiple references to high-risk or sanctioned countries and integrate these insights into risk-based scoring. As a result, financial institutions can achieve more accurate sanction screening and more effective AML monitoring while reducing false positives. Vendors must therefore ensure that their solutions are capable of analysing full transaction data holistically, rather than screening individual parties in isolation.
- **Future-proof design:** ISO 20022's flexible syntax allows additional data elements to be introduced over time. This capability aligns with FATF recommendations for capturing richer originator and beneficiary information to improve AML monitoring, ensuring that compliance systems must be adaptable and future-proof to accommodate evolving regulatory requirements.
- **Targeted system upgrades:** Institutions should have the flexibility to upgrade only their screening capabilities when required, without the need to overhaul the entire compliance infrastructure, such as case management or alert-handling systems. This modular approach helps reduce costs while preserving operational continuity. Modern, API-driven architectures make this possible by enabling seamless integration between screening engines and existing compliance components.

Taken together, these factors illustrate that the richer ISO 20022 data set is not only a powerful enabler of improved compliance outcomes but also a driver of increased sophistication in screening technology and operational processes.

Conclusion and Recommendations

The ISO 20022 migration represents a major step forward for the global payment ecosystem, offering richer, more structured, and standardized data that can significantly enhance operational efficiency, transparency, and compliance processes. The expanded dataset enables improved screening accuracy, reduced false positives, and more insightful regulatory reporting.

To fully realize these benefits, institutions should:

1. **Upgrade screening capabilities.** Implement intelligent **compound matching** logic that evaluates multiple related data points—such as name, city, country, and date of birth—in combination rather than in isolation. This approach enables more accurate scoring of potential matches and hence reduces false positives. Leverage **multi-alphabet processing** to handle non-Latin characters effectively, while utilizing the information contained in both structured and unstructured fields. Make sure that screening takes place against **all transaction data** to avoid any regulatory exposure. This will also allow for **advanced analytics and contextual analysis** such as uncovering relationships between all parties, payment purposes, and remittance details. For example, identifying multiple references to high-risk or sanctioned jurisdictions across the transaction chain can significantly enhance risk-based scoring and improve monitoring accuracy.
2. **Adopt a modular, composable approach.** Where feasible, focus upgrades on the screening function rather than overhauling the entire compliance chain. Use a composable architecture, so capabilities are assembled from interchangeable building blocks that can be added, swapped, or scaled independently. In practice, this means API-first services stitched together through well-defined contracts and event streams.
3. **Design for flexibility and futureproofing.** Ensure compliance systems are adaptable to accommodate additional fields or identifiers that may be introduced in response to evolving regulatory guidance, such as FATF recommendations on enhanced originator and beneficiary information. This adaptability ensures institutions remain aligned with both global and jurisdiction-specific requirements without requiring significant architectural changes.

By proactively addressing these areas, financial institutions can not only comply with ISO 20022 mandates but also leverage the migration as a strategic opportunity to strengthen compliance, enhance contextual understanding of transactions, reduce operational risk, and deliver better, safer, and more transparent financial services to their customers.

HOW TO CONTACT US

If you want to have more information on our solutions and services, please contact us at the following address:

info@neterium.io

Information about our solutions and future events are available on our website

www.neterium.io

The Neterium API is fully documented on our Developer Portal at

portal.neterium.cloud

Follow us on LinkedIn and Twitter/X:



linkedin.com/company/Neterium



[@neterium](https://twitter.com/neterium)

CONFIDENTIALITY NOTICE

©2025 Neterium

Under no circumstances can this document or extracts of this document be communicated to any other third-party without written permission from Neterium.

Neterium SRL disclaims all liability which may result from any unauthorized reproduction or use of the information in this document.

All rights not expressly granted are reserved by Neterium and/or its licensors.

All other trademarks and registered trademarks are the property of their respective holders.

Neterium registered office: 6 Chemin du Cyclotron, B-1348 Louvain-La-Neuve, Belgium.