Navigating sanctions compliance through the transition to ISO 20022

By Benjamin Kelly and Edwin Oloo

The International Organization for Standardization's (ISO) new global messaging standard, ISO 20022, provides a unified language for electronic data interchange between financial institutions that is intended to increase efficiency, lower costs and enhance transparency for the financial system. The messaging format, which applies not only to payments, including real-time payments, but also to securities, trade finance and treasury management functions, should aid institutions in the detection and investigation of potential sanction breaches. However, as institutions work to capture future benefits of the new messaging standard, sanctions professionals and their technology partners should be aware of several challenges the transition poses.

Why is ISO 20022 important to sanctions compliance?

Global messaging standards and the processes supporting them have had to keep pace amid increasing volumes, straight-through processing (STP) demands and evolving regulatory requirements. However, payment messages, such as the widely used Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial information (FIN) service for exchanging message-text (MT) format financial messages, have begun to show their age despite undergoing incremental updates over multiple decades. These platforms were designed when space and bandwidth were constrained and transaction volumes were lower, presenting less of a challenge for manual review processes.

The next evolution in payment messaging is being driven by industry expectations for more streamlined payments messaging (i.e., improved message structures that allow for less variation in the encoding of wire instructions), real-time payments and requirements for payment messaging that better support business, operational, customer, technology and risk mitigation needs. Successful implementation of the ISO 20022 standards will require cooperation across multiple disciplines including but not limited to compliance, IT, operations and analytics. Sanctions-compliance programs in particular can benefit from the richer and more flexible messaging standard, which will allow improved semantic interpretation of payment streams by automated processes such as sanctions screening. Key new and enhanced content standards and structures relevant to compliance functions include:

- Discrete name and address fields for payment parties including debtors and creditors and ultimate debtors and creditors (equivalent to ultimate originator and beneficiary using older terminology), and clear designation of these various payment party roles
- Discrete payment-party identification fields such as birth date and government-document numbers
- Standard codes to indicate payment characteristics, such as payment purpose
- Structured and repeatable remittance fields that provide the ability to describe how the payment should be received by the creditor party (e.g., one payment to be split among multiple subsidiaries of a business entity)
- Support for a wider set of characters beyond those in the Western-oriented basic Latin set.

While ISO 20022 migration should yield several improvements over current standards, achieving them will require careful planning and cautious implementation to ensure that sanctions compliance does not suffer in the process. The changes will likely have implications for compliance staff, as there may be an uptick in sanctions hits for review due to screening of additional fields.

The global payments industry has begun the transition to ISO 20022; however, only payment processing entities have a global-adoption target, set for 2025 by SWIFT. Certain geographies, such as Europe and Singapore, have already aligned regional payment-processing networks to the new standard, while other jurisdictions continue their journey toward ISO 20022 adoption during the two-and-a-half-year coexistence period of existing and new standards that commenced in March 2023 and ends in November 2025. The table below highlights the ISO adoption timelines of some of the key jurisdictions undergoing the adoption process.

ISO 20022 ADOPTION

REGION	CROSS-BORDER	UNITED KINGDOM	EUROPEAN UNION	UNITED STATES	HONG KONG
CURRENT PAYMENT SYSTEM	SWIFT	Clearing House Automated Payment System (CHAPS)	TARGET2	Clearing House Interbank Payments System (CHIPS) FedNow Fedwire Funds Service	Clearing House Automated Transfer System (CHATS)
TARGET ADOPTION DATE	March 20, 2023, with coexistence period through November 2025	April 2023	March 2023	CHIPS: March 2023, with full adoption in November 2023 FedNow: July 2023 (at go-live) Fedwire Funds Service: Full adoption in March 2025[1]	October 2023

Implementation considerations

As institutions progress with implementation of ISO 20022, areas of the business beyond the interface points to the payment networks will be impacted. Compliance officers in particular will need to ready themselves for these changes and consider the following activities to ensure sanctions compliance:

1. **Review all systems and processes that produce, consume or store payment-related information to determine ISO 20022 impact.** While ISO 20022 migration will affect payment messaging-system interfaces, the migration has the potential to also impact an organization's upstream and downstream systems and data stores by way of:
   - Data-element specification changes for existing elements, such as longer field lengths
   - Improved data modeling, such as separate data elements for information that previously would be grouped together into one or more unstructured elements
   - Expanded character set support to include those beyond basic Latin characters, such as those in the Han and Brahmic character set families as well as various Western characters that include diacritical marks
   - Potential new message flows and supporting structures.

[1] The Federal Reserve Banks will adopt the ISO 20022 message format for the Fedwire Funds Service in a single-day implementation strategy on March 10, 2025, with full adoption of ISO also scheduled for that month.

Sanctions compliance programs should conduct a migration-impact review, including mapping changes to the payment flow in and out of sanctions-screening systems and tools. Poor upfront evaluation of ISO 20022 impacts on sanctions-screening systems presents a risk of essential payment-related information bypassing screening processes, potentially allowing for the processing of transactions that should be sanctioned.

2. **Ensure that sanctions-screening testing is integral to overall ISO 20022 migration plans.** With ISO 20022 changes, potentially, hundreds of data elements are eligible for screening. Sanctions-compliance programs will need to plan for detailed, field-level testing that covers each of these intersections with their screening solutions. Testing plans should include not only the typical name-and-address-variation testing across applicable data elements but also verification of matching settings such as match confidence-scoring thresholds, which may no longer be aligned to the institution's risk tolerance. Any new ISO 20022-specific features or enabled functionality identified in the migration-impact assessment should be included in the migration-testing scope. They may include new message flows or organization-specific functionality covered in bilateral or closed-user-group (CUG) agreements or standards.

3. **Verify readiness of sanctions-screening solutions to process the updated payment messaging.** Given the type and breadth of changes identified through an impact review, institutions will need to verify that sanctions screening solutions are prepared to process the updated payment messaging flows or appropriate workarounds are in place to help bridge any gaps. While sanctions screening vendors that process native-format wire data are accommodating ISO 20022, their methodologies may differ. For example, some are introducing new modules whereas others may simply be providing ISO 20022 support as part of an enhancement or upgrade of existing modules. Data-element specifications, payment-data models, potential character-set expansions and new payment-message flows have sanction-screen-system capabilities implications that will need to be confirmed. Examples of review areas include:

    - Instances where payment screening duplicates customer screening due to the unstructured nature of existing message formats resulting in over-screening of certain payment parties
    - Bilateral agreements, CUGs or other special arrangements that may extend payment functionality or structures beyond those defined within the new standard
    - Data elements that may contain characters beyond basic Latin, such as Cyrillic or Chinese, and watchlists these elements will be screened against, along with any transliteration capabilities in the screening solution

- New content, such as that supporting Remittance Information (remt.001), which augments Credit Transfer (pacs.008), which maps to Customer Credit Transfer (MT-103) in the existing SWIFT payment-messaging standard
- Exception lists created for older messaging standards and field structures.

4. **Assess how changes to global sanctions-screening programs will be managed through each stage of the global rollout.** Since not all payment participants will be upgrading to the ISO 20022 standard at the same time, institutions will need to review multiple distinct stages of the rollout and how they will address them. The stages are outlined in the table below.

ISO 20022 ROLLOUT STAGES

YOUR INSTITUTION	OTHER INSTITUTIONS	DETAILS
		PRE-TRANSITION
Pre-ISO 20022	Pre-ISO 20022	Institutions should be actively planning for ISO 20022 migration, which may include impact assessments and confirming vendor upgrade schedules.
		COEXISTENCE PERIOD (MARCH 2023 — NOVEMBER 2025)
Pre-ISO 20022 ISO 20022	ISO 20022 Pre-ISO 20022	While in the coexistence period institutions will need to review how they will address payment-message processing when not all participants are on the same standard. During this period, message-translation services that permit receipt of old and new message formats, such as services offered by SWIFT, can help institutions transition to the new standard at their own pace. However, institutions should not depend on these services existing beyond the coexistence period and will still need to fully transition during this time frame. In the instance where others are already on the new standard, institutions that have yet to transition should review whether sanctions screening adequately covers content on incoming messages that its own payment systems are not yet fully able to handle. In addition, during this coexistence of old and new formats, data truncation will be a risk where content in the new format is being transformed onto data processes still on the old format. For institutions utilizing SWIFT's inflow translation service, they will receive a truncation indicator directly in the MT message content when truncation has occurred so that they may take appropriate action to verify whether there has been material loss of information such as programmatically routing truncated messages for review.
		POST TRANSITION
ISO 20022	ISO 20022	Once all participants are fully on the new standard, institutions may revert to business as usual and, if not part of the initial migration, review whether additional enhancements to take advantage of new ISO 20022-enabled capabilities is needed.

5. **Ensure that STP expectations and sanctions screening capabilities are aligned.** ISO 20022 promises greater STP rates, and thus faster payments, due to improved message structures that support greater automation; however, sanctions-screening processes that are not well-tuned and supported by streamlined review processes may result in a throughput reality that fails to meet expectations for faster processing. As with any major sanctions-screening system change, institutions will need to plan for a tuning cycle to ensure that the screening effectiveness keeps pace with the expected changes. In addition, the sanctions-screening-alert review processes should be reviewed for streamlining and automation opportunities, which could include, for example, secondary scoring and robotic process automation to better enable near-real-time processing.

6. **Educate compliance staff on the usage of ISO 20022-enabled payment messages.** Institutions will need to train staff from all three lines of defense on the implications of ISO 20022. Personnel working on alert reviews and escalations, second- and third-line testing, tuning, and model validation, for example, must be familiar with the new message types, including not only those that are analogs of existing types but also new messages or flows that have no equivalent in existing standards. Training will help staff identify the occurrence of misuse or abuse that could facilitate sanctions evasion.

7. **Remain vigilant for existing sanctions-evasion schemes.** Another promise of ISO 20022 is improved sanctions compliance due to the fielding of information that, in the past, was often in unstructured data elements that could facilitate certain obfuscation schemes or make it difficult to programmatically separate true positives from false positives. However, ISO 20022 won't eliminate all such sanctions-evasion risks, including certain misfielding schemes (for those elements that don't have data-validation constraints) or misuse of message types that may allow obfuscation of the true originator or beneficiary. With more structured content fielding that enables improved semantic interpretation, the ability to perform content-domain enforcement at data entry or detection of misuse or abuse on messages in transit can be enhanced.

8. **Update data-lineage documentation.** Institutions' data-lineage documentation, including data mapping and data flow, should be updated so that data can be traced from payment message to screening solution. This documentation not only will benefit current and future test planning but also is a regulatory requirement in some jurisdictions.

9. **Retune models as part of the migration.** Since the changes to the inputs to the sanctions-screening process may be substantial due to improved fielding of screening-eligible data elements, institutions will need to include sanctions-screening tuning in their migration plans. While payment-transaction screening is the obvious intersection point with ISO 20022, consideration should also be given to other screening inputs if their upstream systems were affected by data-structure changes caused by the migration.

10. **Plan for model validations as part of their migration.** Since the changes to sanctions screening may be significant — impacting not only the data content but also the system configuration — institutions should plan for model validations to be a component of migration. Validations should especially review the screening coverage and scope of testing that has been performed, including any special adjustments to accommodate mixed-message formats during the transition period, to prepare the sanctions-screening model for production.

11. **Expect continued evolution of the ISO 20022 standard.** Some areas of ISO 20022 usage have not been fully standardized (e.g., certain fields may not be initially provided or populated, some payment parties may not be adequately identified, and/or standardized codes may not be used in sanctions-relevant areas such as goods-and-services specification, as has been recommended by the Wolfsberg Group).[2] As such, monitoring programs must not only stay abreast of industry standards and best-practice evolution beyond the initial ISO 20022 implementation but also preemptively monitor messages from other institutions or jurisdictions that are furthest along in their maturity, even if payment systems in their own institution cannot yet fully process the latest standards evolution.

12. **Review whether basic Latin workaround encoding will continue to be effective.** Due to the basic Latin character-set orientation of some existing payment messaging standards, such as SWIFT MT, institutions regularly interacting with payment participants that require other character sets may encounter workaround encodings. For example, Chinese payment participants may encounter or utilize Chinese Commercial Code (also known as Chinese Telegraph Code), which encodes each Chinese character as four digits and permits transmission of this information across payment networks that do not support the Chinese character set. With ISO 20022, SWIFT payments will no longer have the basic Latin character set constraint due to its support for Unicode via UTF-8 encoding. If encoded content is regularly encountered in current payment messaging, institutions should review whether this practice will continue or processes and policies involving these encodings will be outdated and require updating.

[2] ISO 20022 Harmonisation Consultation, The Wolfsberg Group, May 8, 2023, https://db.wolfsberg-group.org/assets/4bcbd5bb-4191-4630-b087-37dc0f48fbb1/ISO%2020022%20Harmonisation%20Consultation%20-%20Wolfsberg%20Group.pdf.

Conclusion

Despite its clear technical infrastructure benefits, ISO 20022 carries implications for compliance personnel and processes. While compliance readiness for ISO 20022 changes will require effort, the long-term efficiencies and effectiveness that the new standard is expected to yield for sanctions compliance and end-to-end payment processing will be a significant boon for the operations of institutions that fully embrace its capabilities.

About the authors

Benjamin Kelly is an associate director in Protiviti's Risk and Compliance practice focusing on technology and data related to anti-money laundering and anti-fraud strategies. He has over 25 years of experience in information technology and business consulting in the financial services industry, concentrating on risk and compliance for the past 17 years. Kelly has worked domestically and internationally in technical-leadership positions for several financial services clients to deliver or support a variety of risk-related solutions, including know your customer/customer due diligence, transaction monitoring, watchlist screening, and integrated case-management solutions. He has been involved with all phases of solution delivery from strategy definition through production rollout and optimization as well as assisting clients with their remediation efforts related to enforcement actions.

Edwin Oloo is an associate director in Protiviti's Risk and Compliance practice specializing in regulatory compliance and advanced data analytics. He has over 10 years of experience building multivariable statistical and machine learning models in the areas of financial crime compliance, anti-money laundering, counter-terrorist financing, eDiscovery, customer risk-rating analysis, risk assessment, fraud, alert risk-scoring, forensics investigations and process automation. He is adept with data privacy laws and building machine learning applications adhering to GDPR requirements. Oloo delivers consulting and advisory services through a quantitative perspective, implementing project management best practices and advanced technical insights while identifying opportunities to integrate data-science solutions. He holds bachelor of science degrees in applied mathematics and finance and a master's degree in data science.

About Protiviti's Financial Crime practice

Protiviti's Financial Crime practice specializes in helping financial institutions satisfy their regulatory obligations and reduce their financial crime exposure using a combination of anti-money laundering/combating the financing of terrorism and sanctions risk assessment, control enhancements, and change capability to deliver effective operational risk and compliance frameworks. Our team of specialists assists organizations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct, and other financial business risk issues.