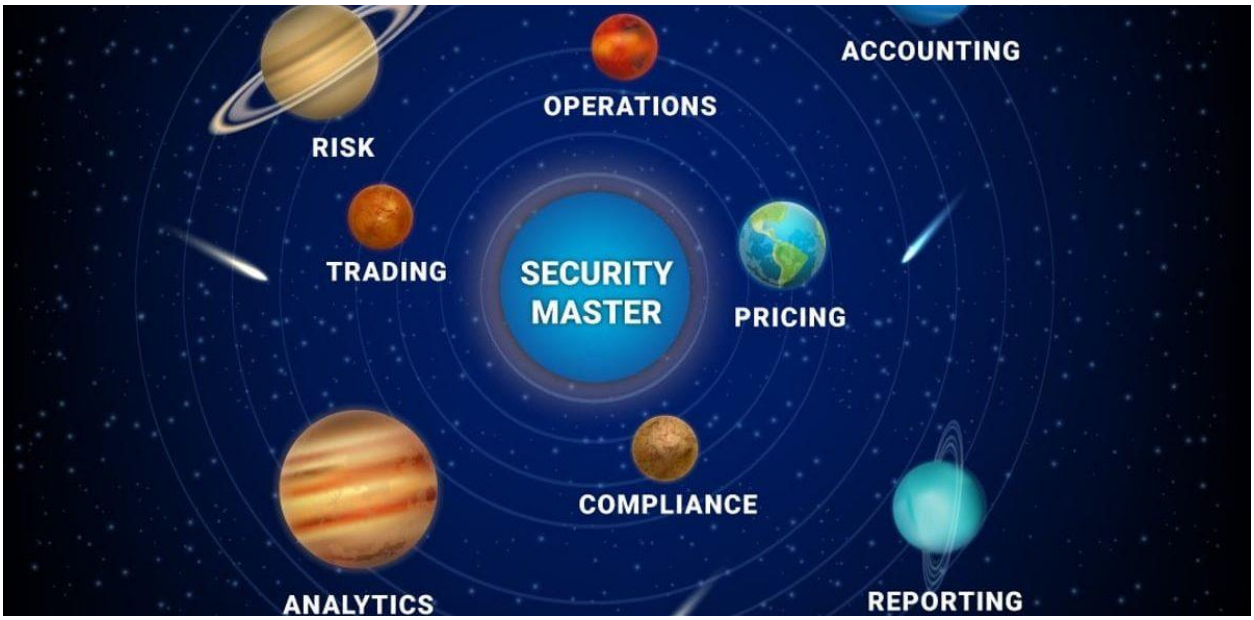

Security Master: The Nexus of the Investment Data Universe

Learn how security master data challenges affect trading and settlement lifecycle, portfolio exposures, analytics, compliance, reporting, accounting and more.

I was talking with a friend a few weeks ago about Grandview and the type of data we work with. This friend had spent many years working with investment data himself but had transitioned to a different industry about five years ago. When I mentioned, “we do a lot of work with security master data,” his response was something along the lines of, “I haven’t heard the term ‘security master’ in years, and I can’t say I miss it!” For those of us who still reside in the world of investment data, we understand the sentiment.

Why does that term evoke such a response? The reason is simple…in the world of investment data, it all starts with the security master. The reference data supplied by this domain sits at the heart of everything your organization will do. It impacts the trading and settlement lifecycle, portfolio exposures, performance attribution, analytics, risk, compliance, reporting, accounting and more. These dependencies lead larger asset managers to devote specialists

to this domain, monitoring and maintaining this data daily and constantly clearing exceptions.

There are many reasons why security master data can be difficult to manage. In this article, I'll spell out some of the most prominent challenges that I've personally come across with clients, while building and/or maintaining it. These are the types of problems that Grandview helps clients solve every day.

1. Defining a "security master"

If you work with this type of data, you likely have a vision in your head of what you think a security master would include. Having partnered with many clients in these discussions, I assure you there are many different opinions on this.

Some organizations may include security analytics under the umbrella of security master; others may include pricing data. In a vacuum, I'd disagree that either of those should be considered part of a security master, but each organization likely has its reasons. For example, it might support some other process to include these types of data in a security master.

Reasonable people and organizations can differ on some of this. What is most important is that within your organization, your reference data strategy defines "security master" in no uncertain terms, and with that, the rest of your data domains as well.

2. Mastering the security master

The refrain that I've heard most often from clients and potential clients about the ideal outcome of their data initiatives is simple: "We want a single source of truth." It makes sense, and who could blame them? I'm certain that some people reading this likely have the same goal.

Investment organizations now consume so much data daily, from a multitude of sources, it's inevitable that decisions will have to be made about which source to choose for a given data point. In the security master domain, the decision to choose one source over another can have wide-ranging implications because this reference data is so ubiquitous throughout all downstream applications.

The security master is critical to every process that an investment manager may run. Where different systems have been procured from different vendors

to perform specialized operations, those systems often will have their own security masters. Vendors often need to package some fundamental reference data architecture with their offerings to support their idiosyncratic functions. Where possible, all these different reference data sets should be aligned to the same security master values.

Security master data management must be a holistic process, performed in a manner that accounts for all the downstream needs of the organization.

3. Asset classes

There is a wide universe of asset classes available to investors in today's investment landscape. Across asset classes there is no single universal set of data points applicable to all of them. Each asset class presents its own data challenges.

The data required to manage an equity portfolio would not be sufficient to support the data required of a bond manager. The needs of those two asset classes are dramatically different. Often, in the architecture of investment systems, you'll see dedicated tables for each asset class because of the wide differentiation of data between them. This presents a technical challenge, but this variation also impacts governance and operating models, ensuring that the proper resources are in place to maintain the integrity of data.

Brand new asset classes come to market regularly. Who else has had to ponder how to model cryptocurrency in a traditional security master? It might be the algorithms targeting me, but I have seen quite a few articles recently about the rise of insurance-linked securities. Some attributes of these instruments are not typically captured by legacy systems and would require the security master to stretch.

Best practices applied to the design and maintenance of a security master will facilitate its adaptability to new and differentiated data. It can be a dynamic data asset.

4. Data granularity

As stated above, the definition of security master is not uniform throughout the world. In the same way, the term "security" may need better definition; for example, some use the term "instrument" instead of "security." Whatever they're called, the data exists at multiple levels of granularity.

Many managers, especially those with narrower mandates, will view the world as much smaller than it truly is. A manager of US equities will likely view Microsoft as MSFT, traded on the Nasdaq exchange. That may be true for them, but it's not a universal truth. Microsoft is traded on numerous exchanges globally. Each of those exchanges have different identifiers and attributes about that specific listing. There are universal attributes about Microsoft that should be shared across all regions and exchanges, but not all data points.

Data providers will not always clearly define the granularity of their data. There are prominent market data vendors that aggregate data in ways that may not align with your organization's needs. The onus for managing this mismatch will largely fall on you.

Your organization's data strategy will define exactly how these different levels of data fit together into a hierarchy, and your security master will be managed as such. Aligning external data to your view of the world may require constant vigilance.

5. Time dimensions

It's tempting to think of security master data as static. For those who have spent years working with this data, who hasn't come across some incredibly wide table in a database, with a single row per security, serving as the security master for that organization? This is a big mistake.

There are at least 2 different time dimensions that security master data must account for:

- **Schedule data**: Attributes about a security which are expected to change over time, and have dates associated with those changes. Sometimes the schedules will be known in advance, sometimes they will be populated as time goes on and events happen. Much of this data falls into the bucket of "slowly changing dimensions," and it requires its own treatment and management. Often, these dates are referred to as "effective dates."

- **Audit data**: Metadata that allows a user to assess the state of the security master at any given point in time. Roughly, it allows us to answer the questions, "What did we know, and when did we know it?" I

like to refer to these dates as “knowledge dates,” but I’m sure someone else might have a better name for it.

Together, these two dimensions are often referred to as bi-temporal representations of the data. Modern data warehousing tools have simplified the mechanics of the audit data piece, recognizing its importance to organizations. However, it is key to define how those pieces of information will be standardized across all data domains and made accessible to the necessary stakeholders.

These are a handful of the general considerations that must be accounted for to have a trusted security master. As you dig deeper, you’ll find more esoteric challenges that may relate to client type (e.g. insurance companies) or specific assets (e.g. alternatives). These challenges will always exist, but adherence to best practices, with a forward-looking mindset and constant vigilance, will minimize their impact on your business. In many ways, a properly managed security master can become an asset to an organization, providing exactly the kind of reference detail necessary to support your view of the world, enhance investment decision-making, and hopefully amplify your competitive advantage.

I started this article joking about how some might recoil at the prospect of assembling a security master. Grandview is not in that group. We are experts in this domain and welcome the challenge. We can help you bring order to your security master struggles and reposition your data to add value to your investment decision making. If you have read something here that hits close to home, get in touch with us, and let’s have a chat about the path forward. Thanks for reading!

ABOUT GRANDVIEW ANALYTICS

Grandview Analytics is a technology consulting and investment data management software company serving financial institutions. We offer data strategy, technology implementation, systems integration, and analytics consulting services as well as an outsourced investment data management and reporting service powered by our proprietary, cloud-based platform, Rivvit.

Our services drive improved business processes, integrated technologies, accurate and timely data, and enhanced decision-making capabilities. Our seasoned team of financial industry professionals brings deep business and technical domain expertise across asset classes and trade lifecycle. With hands-on financial industry experience, we execute on complex initiatives that help clients optimize ROI on data and technology investments.