



**Managing the Security
Master Record**

Managing the Security Master Record

Reader ROI

- Decentralization of security reference data is a challenge for today's managers.
- Firms must allocate time for assessment and planning, for evaluation/development, as well as for implementation of an enhanced system to manage security reference data.

Overview

A fund portfolio manager notices that the sector weightings in the analytical and performance models are different from those reported in the fund's annual report. Isolated instance or common industry problem?

Unfortunately, the scenario is a familiar one and is symptomatic of the challenge facing many investment managers. Over the past several years, rapid business growth has spurred implementation of new applications to support new products and markets. In many cases, the application relied on its own security master. As a result, there is typically no central management of financial security reference data residing in multiple databases across the firm.

The practice of managing multiple security master records drives up the cost of acquiring, validating, maintaining, and distributing information. But, more importantly, without a gold copy of security reference data, the firm cannot be certain that all applications are using the same information.

To correct the situation, firms need to assess and modify their enterprise-wide processes for handling financial security information in light of current and future business requirements. The best-fit solution will depend on the unique requirements of the firm.

Uncovering opportunities

Rather than embark on a series of tactical projects, it is prudent to develop a future-state model toward which the firm can direct change. The future-state model depends on the goals of the firm and its individual business units.

It is important for a firm to understand what current processes preclude the efficient management of security reference data and what improvements can be made to move toward the future state.

To identify pain points in the acquisition, validation, scrubbing, maintenance, and distribution of security reference data, the firm should consider:

- inefficient business processes
- redundant data acquisition costs
- data inconsistencies
- costs of managing technology environments

Since there is no single "right way" to manage security reference data, it is important to review the options that are available. Any solution must be tailored to meet the organization's unique requirements. For example, an option which requires a single point of entry for all new security set-ups will not be appropriate for a firm in which a business unit requires the autonomy to set up its own security records. In such a situation, an option which enables a periodic synchronization with the gold copy would be more appropriate.

Establishing consensus for the future-state operating model among business and technology representatives is another critical piece of the puzzle. A reiterative workshop process which engages key stakeholders may provide the greatest level of success. A vendor-agnostic, workshop-driven approach can surface current-state operational inefficiencies and identify opportunities for improvement. This approach can guide the development of a new process model tied to the firm's goals.

A conceptual architecture tailored to the firm's environment identifies the future-state technology components and data flows. Once the firm has agreed on goals and requirements, it can assess security master vendor solutions. At this point, it is also wise to consider the need to acquire and/or develop software.

The security master vendor evaluation should include:

- solution-benefit
- detailed workflow description of options
- cost
- risk
- scenario build of a high-level implementation plan

Once a solution is chosen it is necessary to develop a business rationale for that solution that includes a return on investment analysis and a roadmap for implementation.

Conclusion

The steps in the planning process cannot be hurried. The firm must allocate time for assessment and planning, for evaluation/development, as well as for implementation of a system to manage security reference data. It is only through a careful, well thought out plan to assess the current state, identify and establish future requirements for the business, and gain consensus from business and technology stakeholders that a firm can streamline its operations and drive economies of scale when managing its financial security reference data.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com