Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Enterprise Data Masking

Securing your non-production data

For most companies the risk of data leakage is a very serious concern. But for financial services institutions, data leakage can result in the violation of data privacy or consumer protection laws. This is even more relevant today when companies are looking to increase profitability in an economic downturn while at risk for being fined by several regulatory bodies.

Financial institutions leverage many security policies to protect and secure data within production environments to minimize these risks. Unfortunately, firms don't always take the same measures in non-production environments such as development and testing. The data leakage risk for these areas may increase as banks, insurers and capital markets firms outsource development and testing projects to service providers who do not have the same stringent information security controls in place.

Using our experience with some of the largest financial services institutions in the world, Capgemini has created a comprehensive data masking solution that provides protection for your data in non-production environments without compromising development and testing efforts. Our solution helps your firm comply with privacy regulations through the use of comprehensive data masking capability which—combined with reporting—supports compliance and audit requirements for regulators.

Data masking is not a one-size-fits-all solution. Data classification can be complicated by the number of data types and changing regulatory requirements. Rather than create a new solution every time, Capgemini brings together the methodology, tools and accelerators needed create a customized solution that meets the unique needs of your financial institution.

Data masking starts with planning & analysis

When designing our data masking framework, Capgemini included domain specialists in banking, payments and cards, insurance, capital markets and risk and compliance to make sure we addressed standards and met regulatory requirements. We developed a robust business glossary to standardize the definition of sensitive data across the organization.

Our custom-built tools streamline the analysis process and help determine a majority of customer/PII data without interaction with your application team. This first broad analysis helps you understand the application landscape and where sensitive data resides, enabling us to score and classify applications according to data leakage risk.

After the first analysis, we establish a clear definition of sensitive data business terms and clarity around the level of risk associated with each term and/or a combination of terms. Data risk scoring is performed using Capgemini's proven data masking methodology so you can identify not only where the sensitive data resides but also which systems are most at risk.

U.S. Regulations

- Basel II Accord
- Fair and Accurate Credit Transactions Act (FACTA)
- Fair Credit Reporting Act (FCRA)
- FDIC requirements
- Gramm-Leach-Bliley Act (GLBA)
- Massachusetts Privacy Law
- Payment Card Industry Data Security Standard (PCI DSS)
- Red Flags Rule
- State insurance commissions

How Capgemini approaches data masking

Data masking is a process where sensitive data is obfuscated to protect it while preserving the characteristics of real data. Data masking is not simply a security or protection method—it is a test data method.

Capgemini's data masking framework is a comprehensive approach that addresses the needs of financial services institutions by providing tools to define, adopt and mature data masking procedures. Our proven methodology helps banks, insurers and capital markets firms define and implement a centralized, enterprise wide solution that supports consolidation, consistency and reusability. Capgemini's data masking solution adheres to two core principles:

- **Masking is not reversible**. There is no way to reverse-engineer the original data from the masked data.
- **Masked data is usable.** For example, when testing valid addresses the masked data must include valid zip codes—not random numbers which fit the data type.

Five Key Components for Data Masking

Classification

Classification is one of the most critical components of a data masking program. It provides focus, guarantees consistent masking and gives upper management the proper tools to mitigate and control risk within nonproduction environments.

Protection

The key driver for a data masking effort is protecting the real data in development and testing environments. When developing algorithms for data masking, we leverage the most secure encryption methods available like AES 128 and 256 bit encryption to protect both the real and fictitious data where it resides—real data in production and fictitious, masked data in development and testing.

Usability

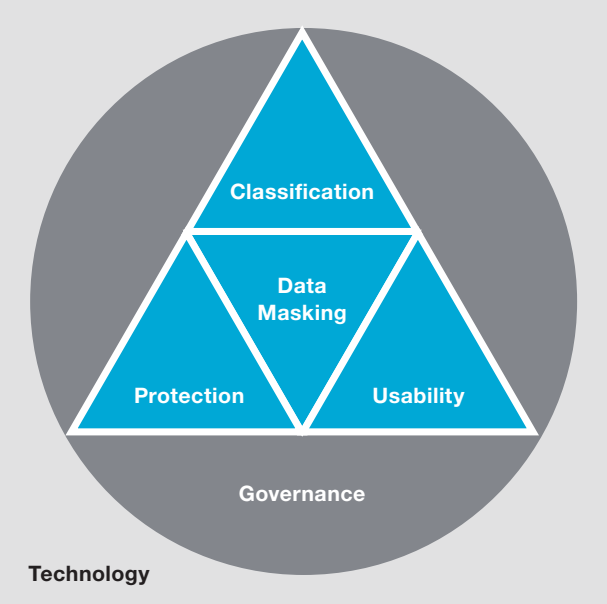
The masked data must be usable in development and testing as substitutes for the real thing. To ensure masked data is usable, we follow these guidelines.

- Masked data should be representative of the source data
- Referential integrity must be maintained so data makes sense in relation to other data
- Not everything must be masked. Data masking should be minimized
- Leverage a robust and flexible set of algorithms

Governance

One of the most challenging aspects of a data masking program is the adoption of the program within an organization. One of the key drivers for this is the lack of ownership. Typically, ownership for a data masking program is spread across different teams and business units within a financial institution. No single party has overall responsibility. For this reason, when starting a program the first step must be to establish governance as a foundation to the program which fosters adoption and addresses ongoing compliance.

Capgemini's Tools & Accelerators for Data Masking



Technology

In our experience, Capgemini has found that establishing strong processes and policies for data masking serve as a solid foundation before selecting a technology. Once these are underway, technology can be leveraged to enable and automate the new processes. Key technologies that enable a data masking program include:

- Algorithms
- Metadata
- Data Profiling
- ETL and Data Subsetting

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.capgemini.com/financialservices

Capgemini's Tools & Accelerators for Data Masking

ALGORITHMS

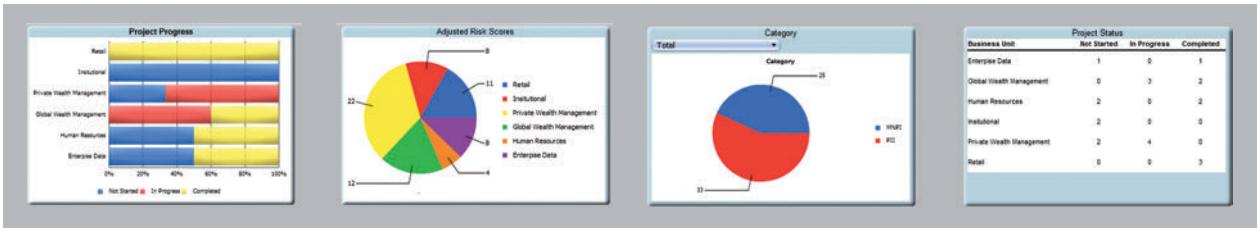
Capgemini has built algorithms to provide flexibility around how the data will be masked and insure that application business rules are not impacted.

- Secure substitution
- Key replacement
- Multiplier
- Randomizer
- Shuffling

Algorithm	Example	Maintain Realism	Consistent	Unique
Secure substitution	John becomes William	√	√	
Key replacement	A21334 becomes X994393	√	√	√
Multiplier	12/31/2010 becomes 3/11/2009	√		
Randomizer	Branch A becomes xxcccmmm			
Shuffling	John→Bill, Tom→John, Bill→Tom	√	√	√

CENTRALIZED REPORTING

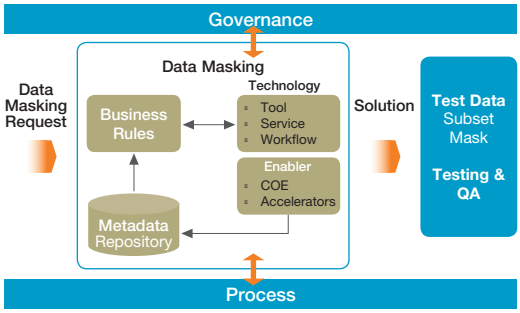
Capgemini leverages a common metadata layer to support operational and regulatory reporting. The centralized data allows for aggregate reporting via dashboards and gives details on what is being masked, down to the table and column level.



TOOL AGNOSTIC ARCHITECTURE

Capgemini's architecture provides a centralized, tool-agnostic framework for data masking. Since data masking leverages common technology like reporting and ETL, our architecture allows you to utilize existing technology investments.

The core of the architecture is metadata which allows for centralized reporting, operational management and scalability.



About Capgemini

With 120,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2011 global revenues of EUR 9.7 billion.

Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.capgemini.com

FS201303040529CS

People matter, results count.