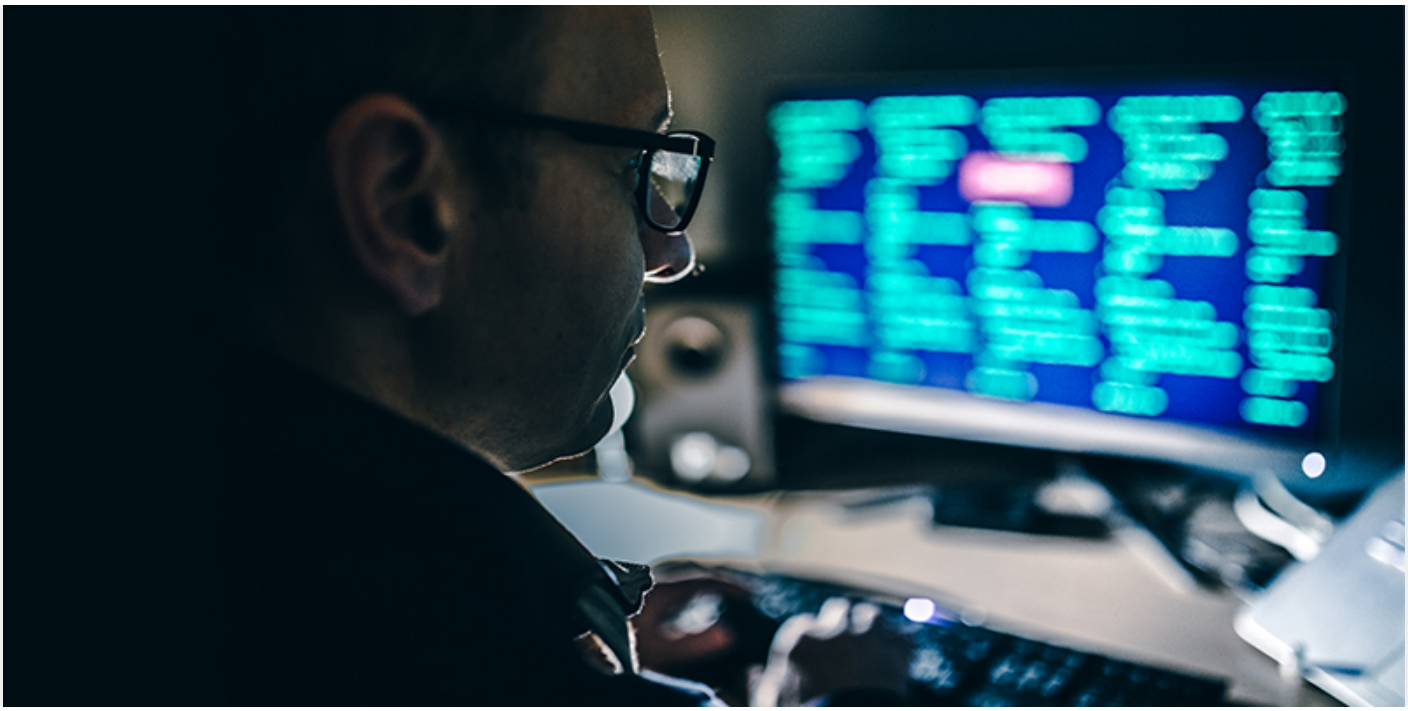
TEST DATA MANAGEMENT STAKEHOLDERS



In Part 2 of this 4-part series, we discuss the stakeholders interested in implementing a TDM strategy.

In Part 1 of this series we discussed TDM and why it is crucial to your organization's success. A robust TDM strategy includes more than consideration of risk mitigation and legal compliance—it must also address the concerns of stakeholders within your organization and those of your customers. Following are some of the roles that may have a stake in what an organization is doing with its test data.

The CIO/CTO. At this level, knowing that there is a positive initiative to always minimize risk and associated costs instills confidence that the organization is handling sensitive data correctly. A TDM strategy will prove accountability and will help to achieve compliance with the local, federal, or international mandates with respect to data management.

The Audit Professional. A TDM initiative verifies that the recommended procedures to achieve management of data are in place. This enables an auditor to easily manage reviews and substantiate the actions taken by the organization to protect sensitive information.

The Security Officer. A TDM system is part of the security mechanisms to protect data and can also provide an inventory of the enterprise assets to be managed under current security guidelines. A TDM system will document how specific data management rules and procedures are defined so that the Security Officer can validate policies at any time.

IT Personnel. Anyone having any kind of hands-on involvement with application development and test data (customer data). Subject matter experts will want to know what is happening to their data.

During a TDM initiative, a plan which describes in detail the phases, activities, and specific tasks and their deliverables to develop processes to protect sensitive data will be produced.

The Consumer. There is a growing realization amongst members of the public who have no tangible connection to the use of personal data that many organizations or enterprises store information about them. Their names, addresses, Social Security Numbers, and more… and they want to be confident and reassured that this data is not going to fall into the wrong hands.

A robust TDM strategy will meet the needs and concerns of each of these stakeholders, in addition to addressing risk of breach and ensuring compliance. In Part 3 of our series, we'll cover the challenges faced when designing and implementing a TDM strategy.