

# TeamWork and Regulatory Compliance

What can dbMaestro TeamWork do  
for your Enterprise



In the past several years, we have all run into the effects of new government regulations in our daily, civilian lives. Last time I went to the doctor's office I had to sign a new form stating I understood my privacy rights with respect to the HIPAA (Health Insurance Portability and Accountability Act). You may also have noticed an increase in the number of mailings from banks and credit-card companies. Most of those include new inserts that outline new and existing privacy notices in order for these institutions to comply with the Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley (GLBA) Acts.

As IT Professionals however, we are confronted by the full brunt of these regulations. Part of our responsibilities is to make sure all those promises of confidentiality and security actual mean something. To wit, safe-guarding our data and procedures and being able to account for who should have access, who actually has access and what changes have been made. The long and short of it is, the more we (as IT Staff), know about our internal data and process, the better.

We, at dbMaestro, took a look at the state of source control and configuration management (SCCM) and saw a glaring hole. While the source code itself was being handled properly, the structure and content of the databases (which go hand in hand with the source) were not being managed with the same diligence. You just couldn't check-in your database into SCCM... Well now you can! TeamWork provides the infrastructure to allow you to integrate your database schema objects and important lookup tables into SCCM.

When it comes to the IT portion of these regulations, a lot of what we have to deal with are the "Wh" questions:

- Who made the change?
- What did they change?
- Why did they change it?
- When did the change happen?
- Where did the change happen from?

In order to comply with the regulations, we need to be able to prove to an auditor that we can provide intelligent answers to these questions for any important bit of customer data (or patient data in the case of HIPAA).



## Sarbanes-Oxley

The Sarbanes-Oxley bill was signed into law in 2002 as a result of corporate wrongdoing, especially the Enron disaster of 2001. The purpose of this legislation was to restore the faith of investors in publicly traded companies by enforcing stricter reporting and disclosure guideline with respect to confidentiality and integrity of financial data.

Section 404 of the law, entitled “Management Assessment of Internal Controls”, is the section that is most relevant to IT Operations staff. Though not specific to the IT world, this section outlines requirements for access controls on corporate financial information.

dbMaestro TeamWork can assist in SOX compliance by providing strict access control to database objects and data. It also provides detailed logging and auditing of changes to the SQL code of triggers, stored procedures, functions, etc. as required by those controls.

## HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 by the U.S. Congress. It established federal regulations that force doctors, hospitals, and other health care providers to meet some baseline standards when handling electronic protected health information (ePHI), such as medical records and medical patient accounts.

dbMaestro TeamWork can assist in HIPAA compliance by helping secure access to database objects and data. HIPAA also requires auditing capabilities on data which can be obtained through TeamWork reporting facilities.

Recent studies have shown that internal security breaches make up a significant portion of data loss and theft. dbMaestro TeamWork allows you to lock your database schema against unauthorized changes and to obtain a complete database audit of authorized changes. TeamWork maintains a complete audit trail of the SQL code of all audited database schema objects.



## GLBA

The Gramm-Leach-Bliley “Financial Services Modernization” act was passed in 1999. The bill was written by Sen. Phil Gramm. Its purpose was to improve the competitive practices in the financial services industry.

Title V – “Privacy” of the act contains language that defines the requirements of these institutions to maintain the privacy of customer and investor data.

dbMaestro TeamWork can assist in GLBA compliance by providing controls on database objects and data that may contain private customer and investor data.

Internal security breaches may negatively affect your ability to maintain privacy controls on investors and customers data. dbMaestro TeamWork allows you institute controls on your database schema objects. By instituting these controls, you can lock the SQL code of your schema objects and maintain a complete audit trail of changes made to the schema objects and SQL code of your database tables, triggers and stored procedures.

### **Our source-code (and now the database schema) should be a part of these controls**

Using our SCCM tools we can show the auditor an accurate audit trail of the changes made to the source-code of our application and to be able to document the Who and What and Where of any given change. Every Check-Out and Check-In can (and must) be documented by the person making the change and so we can pull reports documenting a change trail (e.g. all the changes that were made to a specific module during the last month) and use a diff tool to compare the current version with any previous archived version to determine the exact nature of the change.

dbMaestro TeamWork now extends this concept to objects (tables, views, constraints, stored procedures, et al) inside the database and even the data in the tables. It gives you the ability to perform Check-Out and Check-In operations on these objects and it maintains locking mechanisms so that changes cannot be made with going through the standard SCCM methodology outlines in your corporate procedures. With TeamWork, you can produce the same kind of insightful auditing data regarding changes to your database objects as you have in your other SCCM tools.



For example, the latest revision of your application has been released to QA for testing; they now notice a significant lag in one of the query screens that was not present before. Using TeamWork you can now easily bring up the query and the definitions of the tables and compare them to the previous “faster” version. At this point a simple diff on the DDL will show that an index was dropped from one of the lookup tables which is resulting in slower queries. You also have a full documentation of the person(s) who made the change and the exact time of that change, so you can go back the responsible party for clarification and remediation of the problem.

### **Encapsulation and it's benefits**

When you deploy an application you are usually deploying compiled code. This automatically buys you a level of security because a compiled executable or a DLL or a war file (web application archive) is much harder to hack than the source-code that was used to compile these files. Other parts of your application may also be encapsulated by using compression or archiving, again making them safer and more hacker proof.

Unfortunately, database objects are not subject to the same processing (compilation) and they are deployed into the production environment as simple, plain-text objects. Particularly objects like constraints, triggers and stored-procedures are deployed in plain SQL text and are not protected by any of the benefits of encapsulation. This makes hacking these objects simpler and easier to conceal.

Illicit changes to a trigger or a stored-procedure can be a good way to hack an application. The objects are usually at a very central juncture in the application and changes in them can be used to affect system-wide security breaches. dbMaestro TeamWork helps solve this issue as well. By locking the schema of the database, changes are explicitly blocked unless authorized by an administrator. Any schema changes must now be routed and documented through the TeamWork SCCM process just like any other piece of the application. This allows us to apply our auditing and compliance methodology to these objects.



## In conclusion

These government regulations (and others) have placed an additional burden on IT departments with new policies and procedures that need to be addressed. dbMaestro TeamWork seeks to provide tools to allow the DBAs to integrate procedures to address some of these requirements in the database space. We feel that this segment has not been properly addressed in the past and that our tools can provide cures to some of the issues that plague IT Departments in general and DBA Groups in particular.

In following articles, I will address other issues that impact the database world with regards to SCCM and other topics.

