11g and Compliance

Dan Morgan
Victoria Whitlock

Puget Sound Oracle Users Group (PSOUG)

Introduction

How can you increase the safety and security of your Oracle database while minimizing the cost of regulatory compliance?

In the ever changing world of business requirements IT Professionals need to be aware of the trends and keep up with the resulting changes. No longer can IT Professionals hide in the back room and ignore the changes in regulatory requirements. IT professionals are now able to become full partners with the business and provide valuable insight as well as reducing risk, both financial and regulatory. One of the issues is the rapidly changing business environments caused by changes across emerging markets, new technologies, business relationships, regulations, and competitive pressures. This white paper is meant to offer options, as each business has specific needs and requirements. We will review some of the new features that can make a difference in how you implement solutions to regulatory needs.

Oracle has many options for enforcing compliance requirements. Some have been around for many years, such as complex passwords and password complexity. Others are newly released and back ported to version 10.

Common Regulatory Requirements

The common press has tales of lost data, stolen personal identifiable information (PII), and other misadventures. The increased awareness and concern at all levels means that IT Professionals need to understand the business case for the increased demand for security and data protection.

The most notable regulatory requirements come from the Sarbanes – Oxley Act of 2002 (SOX), Health Insurance Portability and Accountability Act of 1996 (HIPAA) , Payment card industry requirements(PCI), Gramm-Leach-Bliley Act of 1999(GLBA), Fair Credit Reporting Act 1971 (FRCA) and The Fair and Accurate Credit Transaction Act of 2003 (FACTA). These are just a few of the regulatory requirements that companies have.

One of the most common misconceptions is that we in the United States are the only ones who face such regulatory requirements. Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA) 2004, the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, and the Japanese have a version of SOX called the J-SOX: Financial Instruments and Exchange Law

If we take a look at each of these regulatory requirements you will see that many items are similar and you do not need a separate compliance program to fulfill the obligations of each.

1. SOX requires you have controls around your financial transactions, this includes the computer controls as well.
2. HIPAA requires the adoption of security and privacy standards in order to protect personal health information.
3. GLBA provides limited privacy protections against the sale of private financial information, codifies protection against “pre-texting” to obtain personal financial information through false pretenses and allow consumers the right to opt out from limited “nonpublic personal information”.
4. FACTA requires the safeguard integrity and accuracy of collected and disseminated data as well as the safe disposal of information derived from credit reports.
5. PCI is not a government regulation, it is an industry standard, it is meant to protect credit card information and prevent misuse of such information.

Figure 1 is a visual overview of the common requirements; but not a complete or exhaustive list.

Figure 1

Regulation	Access Controls	Data Retention	Data Security	Encryption Requirements	Auditing
SOX	X	X	X	X	X
HIPAA	X	X	X	X	X
FACTA		X	X		
PCI	X	X	X	X	X
GLBA	X	X	X		X

As business drives the IT requirements this is an opportunity for IT to provide options to business to reduce the cost of compliance by using tools already available in the Oracle product set. Some of these tools are without charge such as password complexity which has been part of the Oracle database since Version 8 and is free. Others can be licensed for an additional cost and training should be taken to take advantage of the new features such as Audit Vault.

Oracle Database Features

Project Lockdown it is an Oracle resource that is very valuable. It is a step by step methodology to secure your database infrastructure. The concept is simple, a security audit is looming and you need to harden your infrastructure and still continue with your "real" work. The information in project Lockdown is relevant to Oracle versions 9.2.0.x (Oracle9*i* Database Release 2) through 10.2.x (Oracle Database 10*g* Release 2). Project lockdown can be accessed at:
http://www.oracle.com/technology/pub/articles/project_lockdown/index.html

Almost all Database Administrators login with SYSDBA, that is one privilege that should be tightly controlled. One option is to make a Daily DBA role and assign it activities that DBA's do on a regular basis. Another is to limit who on the DBA team actually has the ability to login to the production environment with SYSDBA.
Passwords are a common requirement for accessing Oracle and other applications. Prior to Oracle Database 10*g*, the password is not prompted to be entered during RapidInstall, thus the default password—e.g. "change_on_install" for SYS and "manager" for SYSTEM—were left active. In a recent survey of Oracle Databases 35% still had default passwords. The survey was limited to 100 installations and within the United States. Ensuring that your passwords are changed and accounts that are not used are locked is one easy step to minimize compliance risk.
One of the most popular hacker tricks is to inject a large amount of text into the Listener, causing the Listener it to go down. The database could be still up, but since the Listener is down, no new connections can be established—which in effect is a "denial of service" attack. Password protecting your Listener is an easy and simple task to minimize a "denial of service" issue. After you have instantiated a password on your Listener you should review your log files to determine if someone is attempting to change your parameters online.
Oracle has had the ability to audit users since version 8, however the overhead is significant if you are not judicious in your choices. With the audit option you may want to audit just the login attempts to determine who is getting a logon denied error. If you have a user that is failing to logon after a significant number of attempts, you may have someone attempting to hack your system. Be aware the audit trail is written to the SYSTEM tablespace by default so you may want to create another tablespace for the audit trail and/or watch the space consumption.
Another area of concern is sensitive columns with obvious names such as Salary, Social Security Number or Birth date. In Oracle version 10, you have the option to mask the column names; virtual private database (VPD) (also known as fine-grained access control) provides powerful row-level security capabilities. VPD works by modifying

requests for data to present a partial view of tables to users, based on a set of defined criteria. When a user directly or indirectly accesses a table, view, or synonym protected by a VPD policy, the server dynamically modifies the SQL statement of the user. The modification creates a WHERE condition returned by a function implementing the security policy. VPD policies can be applied to SELECT, INSERT, UPDATE, INDEX, and DELETE statements. VPD has the ability to support a variety of requirements, such as masking columns selectively, based on the policy and applying the policy only when certain columns are accessed.

Oracle Enterprise Manager Data Masking Pack in 10g also offers a wide variety of options to mask data. The Data Masking Pack uses an irreversible process to replace the sensitive, PII or confidential data with realistic-looking but scrubbed data based on certain rules. The process is so complete that the original data is unrecoverable. The original data can be replaced with nonsense data or if realistic data is required, for example names and addresses, the data can be replaced with outside source data.

Encryption is a valuable tool as a last line of defense, it is not enough alone to show due care. Data is accessible to the user but only with a key. Without the key, the data is useless. You must protect the key; if someone gains the key they will have access to your data.

Oracle provides two types of encryption:

1. Encryption APIs such as the packages dbms_obfuscation_toolkit and dbms_crypto (in Oracle Database 10*g* Release 1 and later). Using these packages you can build your own infrastructure to encrypt data. This is the most flexible approach, but rather complex to build and manage. The dbms_crypto is a much more usable and better utility than dbms_obfuscation_toolkit, which is harder to use and manage.

2. Transparent Data Encryption , a feature of Oracle Database 10*g* Release 2 and later, obviates manual key management. The database manages the keys but as the name suggests, the encryption is transparent—data is stored in an encrypted manner only.

Regular encryption is the only type available prior to 10g Release 2. Regardless of the type of encryption used you must identify the tables, and more specifically the columns, to be encrypted. The cost of CPU cycles can get to be extensive, so only encrypt what needs to be encrypted.

The following table may help in deciding which package is a better fit for your organization. Figure 2

	Transparent Data Encryption	User-built Encryption

Flexibility	Minimal—For instance, if the column SALARY in SALARIES table is encrypted, then *any* user with access to the table will be able to see the data clearly. You can't place selective control on that column based on user roles and levels.	Robust—For instance, you may define the column to be shown in clear text *only if* the user is a manager; and encrypted otherwise. This will ensure the same application sees the data differently based on who is using them. This flexibility can also be expanded to other variables, such as time of day or the client machine accessing the database.

Setup	Minimal—This facility is truly transparent—there is nothing to do but issue this command (provided all other one-time jobs have been executed, such as building the wallet):
	`ALTER TABLE SALARIES`
	`MODIFY (SALARY ENCRYPT)`
		Extensive—To provide a seamless interface to the users, you have to create a view that does a decryption of the column. This view should then be granted. This introduces several layers of complexity in management.

Key Management	Automated—Key management is handled by the database, using a wallet.	Manual—Since you have to manage the keys, you have to decide how you can balance between the two conflicting requirements: • Make the key secure so that it's not accessible to an adversary • Make it accessible to applications
Restrictions on columns	Some—Certain columns cannot be encrypted, such as those with partition keys, of data types BLOB, etc.	Only restriction is LONG.
Support for indexes	N/A—Indexes may not help in queries since the data is stored in an encrypted manner.	Yes—Since you control the encryption, you can create surrogate columns to build indexes on.

Conclusion

You can minimize the cost of your regulatory requirements if you take the time to understand the features that Oracle provides you.