The Feds Are Watching

A modular IT framework positions you to cope with today’s regulatory deadlines—and new mandates on the horizon p32

CLICK HERE
For a Free Subscription
The Feds Are
“Hurry up” is the latest battle cry at companies struggling to fall in line with an onslaught of government regulations. The summer of Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), and other mandates is upon us as deadlines loom. The heat is beating down on IT administrators, whose chief executives face stiff penalties — even jail time — if their companies fail to comply with the law.

“The frightening big stick of enforcement is out like a brick bat,” warns Lane Leskela, research director at Gartner. “There’s a lot of confusion around implementing regulatory compliance as a process.”

Part of the confusion stems from the sheer number and scope of regulations affecting companies that, until recently, took an application-specific approach to regulatory compliance in an effort to cope with individual mandates.

By Richard Ginzel | Photograph by Robert Daly
Enterprises are beginning to see the futility of that strategy, which results in fragmented processes ill-equipped for the next body of mandates that comes down the line. Instead, business and IT are joining together to create extensible compliance frameworks that can accommodate any number of regulatory mandates, providing componentlike reusability that simplifies change management and reduces deployment costs.

“Sarbanes-Oxley, the Patriot Act, and HIPAA were the straws that broke the camel’s back, and companies are saying, ‘We’ve got to find a better way to do this — the regulations are only going to get worse,’ ” observes Ted Frank, CEO of Axentis and advisory chairman of The Compliance Consortium, an industry group formed in June to help CIOs and IT outfits get organized. The consortium’s mission includes making sense of all the overtures from vendors who are in gold-rush mode.

The high anxiety is fueled by what Gartner’s Leskela calls “the lack of a consistent technology approach to managing governance, risk, and compliance processes across the board. It’s a very complex environment.”

**Looking Out for the Law**
Consider just a few of the systems that fall under the monitoring provisions of Sarb-Ox: data security, disaster recovery, content management and archiving, information retrieval, transaction surveillance, and e-learning (the ability to deliver ongoing education online). Section 404 of Sarb-Ox will put a huge burden on IT by requiring companies with valuations of more than $75 million to prove that their internal controls and audit trails are sound and that their processes are capable of producing certifiably correct data. And, ready or not, Sarb-Ox’s infamous Section 409 — which mandates that “material events” such as the acquisition of a big customer, or anything that could affect a company’s perceived market value, must be reported within 48 hours — is upon us, taking effect Aug. 23.

The liability doesn’t stop there. Many enterprises remain unaware that Section 215 of the Patriot Act requires companies to surrender customer data when subpoenaed and gives customers the right to sue if they haven’t been properly warned that their information will be disclosed if the feds ask for it. Then there’s the HIPAA Final Security Rule, which will take affect in April 2005 and will grant individuals the right to sue organizations that allow a security breach to expose medical records.

The good news, experts say, is that separate regulations bodies have many directives in common — the call to retain IM exchanges and e-mail, for example — thereby enabling IT to create a modular compliance framework. Most companies already have systems that employees and consultants can leverage and integrate into a wider compliance strategy.

“If you understand the consistencies of these processes within your company, you can build a scalable technology infrastructure while leveraging existing investments,” Axentis’ Frank says. “Just because you put together a strategic framework doesn’t mean you need to full-out implement it right away across all processes. If you can develop a baseline plan, you can still act tactically.”

Ultimately, two frameworks are required: one for business and one for IT. The business side needs to develop a management infrastructure to establish and maintain internal controls and repeatable processes that ensure reliable regulatory compliance. IT needs a technology framework that capitalizes on existing resources and makes point solutions the exception rather than the rule.

**Building Better Management**
Government regulators don’t explicitly tell enterprises how they should reorganize for compliance. But in June 2003, the Securities and Exchange Commission implicitly recommended the Com-
mittee of Sponsoring Organizations (COSO) of the Treadway Commission framework. COSO, an independent auditing industry group established in 1985, released a seminal report in 1992 entitled “Internal Control — Integrated Framework,” which describes how companies should establish and maintain controls to avoid fraud. But the COSO framework seeks to help organizations develop proper business processes, mainly related to authorizing and reporting transactions, not to creating controls that apply specifically to IT.

Instead, many IT execs are turning to the COBIT (Control Objectives for Information and Related Technology) framework for help. Published by the IT Governance Institute, COBIT provides guidelines for IT security and control. The organization’s “IT Control Objectives for Sarbanes-Oxley” (infoworld.com/1678) details IT’s role in implementing and sustaining control over disclosure and financial reporting, including planning, acquiring missing pieces of technology, properly deploying solutions, and monitoring compliance.

The larger the company, the more likely it is to have implemented the controls outlined by COSO and COBIT and to have adjusted management structure accordingly. As regulatory deadlines approach, small and midsize companies will face the greatest risk.

“We’re encouraging smaller companies to form a committee and put a virtual team in place,” says David Donelan, senior director of industry and compliance solutions at EMC.

According to CJ Rayhill, CIO of O’Reilly Media, without a cohesive team, “you typically have one person who is anointed as the expert. So, in addition to their day job, they try to make sure everyone else is in compliance — and it’s mostly hit or miss. The biggest issues I’ve seen are around authority. At big companies, [compliance officers] have a direct line to the CEO. In smaller and midsize organizations, a perceived lack of authority can make it more challenging to get people to respond to compliance efforts.”

Gartner Research Director Brian Wood advises companies to create the position of CCO (chief compliance officer), who would report to the board and be equal in stature to the CEO, rather than report to the CEO. “I’m sure Mr. [Ken] Lay can see the reason for that,” he says. Wood believes the CCO should install a rotating IT representative to assess existing IT assets, to validate processes, to meet security needs, and to ensure that there are clear methods to address abuses. Why rotating? “It helps more and more people get trained in compliance and works toward a cultural change within the company,” he says.

The IT and legal departments — or outside legal counsel — also make up a crucial alliance, according to Deidre Paknad, CEO of PSS Systems, a provider of document policy solutions. “There needs to be more dialog between the two. Compliance is, at its heart, a legal issue — and then an IT issue. But they all think the other speaks a different language. They need to dine together more often. There should be frequent discussions about the synchronization of information to reduce companies’ risk.”

Risk assessment comes into play at every turn. “Our advisers have given us 3-inch [thick] binders of what to do. But the question is always, ‘Where do we start?’ ” says Wood, who is also a member of Gartner’s internal compliance team.

Wood says to start by assigning risk levels to systems, processes, and personnel that are susceptible to breaches and then assess the consequences of those potential breaches. From there, you can use those assessments to make a priority list for implementing systems and controls. According to Wood, using that criteria makes it fairly easy to come up with the top 10 things your organization should be working on.

---

**Compliance From the Ground Up**

A flexible CPM (corporate performance management) architecture includes software for document and records management, along with an automated BPM component.

---

**Source: Gartner**

NOTE: Not intended as a comprehensive list
**Marshalling the Right Technologies**

IT is charged with implementing the systems that allow process owners to know “what information we have, where it is physically, which systems have possession of it, which rule settings are applied, and where I go for answers when risk arises,” PSS’ Paknad says. Of course, the precise systems vary widely, but the efficient retention and disposal of information in accordance with a single system of records is crucial when an audit or a request for discovery occurs, she says. Document and records management — along with effective management of information lifecycles — are the foundations of a sound compliance architecture (see “Compliance From the Ground Up,” page 35).

Creating a modular, extensible IT compliance framework starts with storage hardware. Document management, e-mail archiving, security, and BPM software all have vital roles to play — and should be equipped with monitoring and change management capabilities. Yet the law seldom mentions specific technologies. Regulations typically don’t dictate which storage medium should be used. For example, Section 802 of Sarbanes-Oxley stipulates that records be stored for seven years, during which time they must be nonerasable and nonrewritable. “So to us that means WORM media,” notes Charles Brett, vice president at Meta Group.

But WORM needn’t mean that enterprises pony up for slow and expensive optical disc solutions. “For a compliance infrastructure, companies are now looking at highly scalable storage such as EMC Centera … and getting away from point solutions by departments” such as those involving magneto-optical drives, Brett says. Offering WORM storage on magnetic disk, the EMC Centera Compliance Edition combines ironclad storage software with a capacity that starts...
at 5TB. It supports real-time replication for fail-over redundancy and has an open API that allows for integration with dozens of compliance applications. Perhaps the biggest plus is the policy-based archive features, along with search and index functions that support fast data retrieval.

EMC’s chief competitor in this space, IBM, sells the Data Retention 450. In the context of IBM’s wide array of middleware and network management offerings, the Data Retention 450 can be thought of as the WORM component of a huge content- and data-retention suite. As does EMC, IBM offers policy- and event-based storage management with compliance in mind.

The next piece of the puzzle is document management software, which ensures that information is identified, indexed, and labeled at its point of origin and then is sent to the appropriate storage medium. Leaders in this space include Documentum — recently bought by EMC — and FileNet, which offers Content Manager and Records Manager as part of its FileNet Compliance Framework. A document and information policy management application, where policy and rules settings can be changed to meet different regulations, comes with PSS Systems Atlas IPM (Information Policy Management) suite.

Thanks to a few high-profile fraud cases, e-mail has emerged as an infamous liability. The archiving of e-mail — and more recently, IM — has received much attention from vendors such as Legato, which was bought by EMC last year, and from several specialty archiving software providers, including iLumin and KVS. Along with its shrink-wrapped product, EAS (Exchange Archive Solution), e-mail archive provider Zantaz provides a hosted solution called Digital Safe Service.

Such offerings ensure that e-mail and IMs are indexed in real time, while allowing IT to set up rules and policies that allow for sophisticated searches and timely retrieval.

Security and identity services play a critical role in proving that the information being committed to record is valid (see “Covering Your Assets,” page 38). “If your systems themselves aren’t secure, then what good is the information from those systems?” Gartner’s Wood asks. “But this is a case where enterprises already ought to have systems in place before compliance issues are even considered.”

Rick Caccia, director of product management at Oblix, producers of CoreID identity management software, acknowledges that the company has no specific compliance offering and that many IT outfits are leveraging existing security systems. “But we can automatically generate audit trails for the applications we protect,” he says. “So, it becomes useful in the compliance arena, where a lot of the language in the regulations, particularly Sarbanes-Oxley, is pretty vague when it comes to defining effective controls.” In the end, security tends to become distributed across the framework by access-control limitations placed on a variety systems.

**Leveraging Existing Assets**

For every compliance need there is a vendor. But to avoid needless spending, industry groups stress the importance of making a top-to-bottom assessment of IT assets before writing any checks. That way you can determine which assets can be folded into a compliance framework. “The No. 1 thing you want to do is take inventory so you can look at what you have and figure out whether or not it can be repurposed,” says John Haggerty, vice president of AMR Research. “A company already heavily invested in document management can bypass those potentially costly solutions, whereas some other company may have to go outside and find a vendor to assist in that area.”

According to analysts, the biggest piece typically missing at small and midsize companies is the BPM component. BPM software demands extensive application integration, but after BPM is implemented, IT can string together workflows across existing applications, making the most of applications already in place. BPM vendors such as IBM, Lombardi Software, Intalio, and Savvion all provide the tools needed to create enterprise-spanning compliance solutions. “If you can’t validate the process by which you gathered the

**Regulation Rundown**

A wealth of compliance resources awaits you online.

- American Institute of Certified Public Accountants aicpa.org
- The Compliance Consortium thecomplianceconsortium.org
- Compliance Pipeline compliancepipeline.com
- Compliance Week complianceweek.com
- Health and Human Services, Office of Inspector General oig.hhs.gov
- Jefferson Wells International www.jeffersonwells.com
- Open Compliance and Ethics Group oceg.org
- U.S. Sentencing Commission ussc.gov

According to analysts, the biggest piece typically missing at small and midsize companies is the BPM component. BPM software demands extensive application integration, but after BPM is implemented, IT can string together workflows across existing applications, making the most of applications already in place. BPM vendors such as IBM, Lombardi Software, Intalio, and Savvion all provide the tools needed to create enterprise-spanning compliance solutions. “If you can’t validate the process by which you gathered the
information, how can you validate the information?” asks Chris McLaughlin, director of product marketing at FileNet, which equips its software with BPM-like capabilities. “That’s what Section 404 is all about. Content management only addresses half of it.”

Big players such as Microsoft, SAS, BMC, SAP, and PeopleSoft have entered the field to provide compliance solutions, while Nth Orbit, Movaris, HandySoft, OpenPages, and Paisley Consulting continue to provide specialized offerings. But analysts and even some vendors caution IT shops to be wary of anyone promising an end-to-end solution with unmatched sophistication. “No one can give you compliance in a box,” PSS’ Paknad asserts.

Jeff Lundberg, senior product marketing manager at Veritas, urges IT to “look for solutions that provide features and functions that can be adapted as regulations change and new ones come into play.”

That may be difficult, as companies scramble to meet deadlines. An April 2004 survey by the Institute of Internal Auditors reported that a mere 2 percent of respondents said they were ready for Section 404 certification this November. No doubt point solutions will be slapped on in some cases instead of extensible ones. But after the dust clears, the companies that deploy framework-based technologies will ultimately enjoy an overall increase in IT flexibility, rather than simply staving off the long arm of the law.

Covering Your Assets

As components of your compliance framework expand, their functions spread across an array of IT systems and business processes.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Security and identity</td>
</tr>
<tr>
<td>Audit</td>
<td>Business process management or portals</td>
</tr>
<tr>
<td>Approval, status, and escalation</td>
<td>Records, knowledge, document, and content management</td>
</tr>
<tr>
<td>Intra-application routing and workflow</td>
<td>Integration broker suites</td>
</tr>
<tr>
<td>Interapplication routing and workflow</td>
<td>Business continuity management</td>
</tr>
<tr>
<td>Content storage presentation and scripting</td>
<td>Business activity monitoring</td>
</tr>
<tr>
<td>Data and metadata management</td>
<td>Corporate performance management</td>
</tr>
<tr>
<td>Process and control documentation</td>
<td>Forecasting</td>
</tr>
<tr>
<td>Analytical reporting</td>
<td>Planning</td>
</tr>
<tr>
<td>Collaboration</td>
<td>Budgeting</td>
</tr>
<tr>
<td></td>
<td>Consolidations</td>
</tr>
<tr>
<td></td>
<td>Reporting</td>
</tr>
<tr>
<td></td>
<td>Financial management systems</td>
</tr>
</tbody>
</table>

NOTE: Not intended as a comprehensive list

SOURCE: GARTNER
Keeping Data Confidential

Prying eyes can cost companies big time, especially when medical records are exposed. These techniques for obscuring database records can help

Many companies that were doing business in a relatively carefree fashion a year ago now find their customers insisting on high levels of accountability. Of course, health-care organizations have been under the watchful eye of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the Health Insurance Portability and Accountability Act (HIPAA) for quite some time. But public companies outside the health-care industry have woken up to find themselves facing Sarbanes-Oxley and other mandates. And in April 2005, HIPAA’s Final Security Rule will kick in, exposing organizations to potential lawsuits if medical records are exposed — even when as a result of skillful hacking.

Each of these regulations requires enterprises to protect and control the flow of information. Strong, identity-based access-control systems accomplish this for applications and resources, but when it comes to databases — against which

By Sean McCown | Illustration by Ben Barbante
you can’t know whether a database is truly secure unless you know what data has been accessed, how it has been modified, and who has viewed it. Entegra – an enterprise-level auditing tool for SQL Server (and soon for Oracle) – can tell you all these things. And it does so in a way that’s easy to implement, that’s highly scalable, and that minimizes the impact on database performance.

Entegra audits all SQL activity, including inserts, updates, and deletes, as well as changes to database schema, access permissions, and views. It uses agents to collect these activities at scheduled intervals, stores them in a central repository, and provides a Web browser interface to view reports. Entegra can also send e-mails and other alerts in response to events that you specify; for example, if a table schema is changed or an entry in a table is deleted, any number of administrators can be notified.

Auditing not only gives you a solid measure of your success but it also provides you with an added layer of security.
these methods and just encrypt that data in the database itself. This comes at a cost — not only does it take extra time to write the record, because it has to pass through the encryption routine, but you also have to buy an encryption routine. These typically aren’t cheap, and unless you have a cryptologist on staff, you may find yourself in the middle of a very expensive solution. Using encryption has one major advantage, however: With all the other methods, anyone who knows the database schema can bypass the mechanisms you’ve put in place and query the data directly. This isn’t possible with database-level encryption.

**Use Your Imagination**

When it comes to obscuring data from users, you can seldom be too creative. Remember that data obscurity is a security measure and that good security never has a single point of failure. You would never see a network where a firewall or a router or a simple password policy was the sole security measure. So, just as your network makes use of many levels of routers, firewalls, access policies, and passwords, your database should have multiple levels of security.

When it comes to securing data, I live by a simple philosophy: Treat everyone as a potential criminal. Threats come from both sides of the firewall. You never know when a disgruntled employee might do malicious damage to the network or walk off with a copy of a database backup. These are real possibilities that must be considered — not only for your company’s own needs but also to protect your customers from the fallout of having their sensitive data exposed.

With internal threats in mind, another common method of obscuring data is to create a separate reporting database, possibly even on a separate server. An ETL (extraction, transformation, and loading) tool can be used to publish data to this separate database and transform it along the way. This may be the most secure of all the meth-
By now it should be clear that the best No Single Solution

The key is kept in a different location. no matter how closely they look at it.

system is real to everyone who sees it,

This way, everything in the production pull the real records back out again.

Another crafty technique is to create routines that insert extra data as a smoke screen to confuse anyone who gains access to your database. By keeping a pool of fictitious names, phone numbers, and so on, you can generate random false records, making it impossible for even a disgruntled insider to determine the accuracy of any given record.

I implemented this solution for a major health-care organization, and it worked very well. Even the biostatisticians couldn’t spot the fake data. I also created three false records for every real one, which greatly diminishes the likelihood of a thief finding a real record. Separating the genuine records from the bogus ones simply becomes too much trouble.

So how can the system administrators tell fake data from real data? Well, obviously you have to plan ahead for that one. There are two basic methods for separating the data back out. One way is to create an extra column that provides some kind of control. This column can be encrypted, or it can be a bit flag with an ambiguous name.

However, I prefer to not have anything in the database that might allude to the fact that all the data isn’t real. Rather, I prefer to create records in another system and then use a join to pull the real records back out again. This way, everything in the production system is real to everyone who sees it, no matter how closely they look at it. The key is kept in a different location.

No Single Solution
By now it should be clear that the best plans for securing data will combine several of these methods.

For example, you can use stored procedures or UDFs that call encryption routines, but UDFs by themselves aren’t effective because users might not wrap the column inside the function. You should give users a view to query and write the view so that it wraps the columns inside the UDF. This way, users can still perform ad-hoc queries on the data, while administrators maintain control over what the users see.

If you are adding dummy data, views can be used to conceal that fact from your users. By creating the view with a join against a foreign table that filters out the extra data, you can create an additional level of obscurity. This same technique could be deployed as a stored procedure as well. If you employ this method, don’t forget to run your fake data through the same encryption routines as your real data. It completes the illusion. And of course, if you don’t publish your schema, your users won’t be able to bypass your measures, because they won’t know what tables to query.

When I was brought in to lead the compliance effort for a major hospital chain, I entered a culture in which all the system administrators and analysts had enjoyed complete access to all the clinical databases for years. They were very familiar with both the schema and the data itself. It forced me to build another schema that summarized the data for the analysts and loaded it every night from the production systems. This schema resided on a different server, in another building, under the control of an outsourced datacenter. The administrators and analysts were then locked out of the production systems, and the backups were encrypted to protect against theft from outside. In this case, it wasn’t necessary to encrypt anything because sensitive data simply wasn’t being brought over to the reporting system.

Monitoring the Results
After putting your plan in place, you still need to measure your success. Auditing is the best way to achieve this. I’m not going to lie to you; a complete, enterprise-level auditing solution is not cheap, and depending on the database you have, you may never find a perfect solution. That doesn’t mean you shouldn’t try — auditing not only gives you a solid measure of your success but it also provides you with an added layer of security.

Unlike some security measures, you need not keep this process under wraps. In fact, if users are aware that their database activity is being audited and that there are severe penalties for tampering, they’re far less likely to try to circumvent your plan. Oftentimes

Countdown to the HIPAA Time Bomb

Companies have until April 21, 2005 to ready their databases for HIPAA. So what can database administrators do to ensure compliance?

- Determine which data can be considered sensitive.
- Perform a risk analysis and document justifications for decisions made.
- Determine security measures based on identified danger levels.
- Establish metrics for success, such as proof of thwarted real or simulated attacks.
- Audit not only changes to each system, but who has access to data.
- Encrypt backups for off-site storage.
this is all it takes to raise the integrity level of your staff. You can even keep your auditing costs down by using what I like to call the dog-training approach.

If you’ve ever bought those electrified mats that shock your dog when he walks across them, you know what I’m talking about. The mats have a pattern on them, which the dog learns to associate with the shock. When you buy the mats, they sell you dummy mats as well. The theory is that the dog will learn to not walk across anything with the mat’s pattern.

Auditing works the same way. Audit your major systems, but tell your employees that all the systems are under full audit. This should give you the best of all worlds: Your company is fully compliant, because the major systems are audited; you didn’t have to actually pay to audit all the systems; and you have the most honest employees around.

Flexible and Granular Database Protection

DbEncrypt allows you to apply column-level encryption in your SQL Server database and assign view permissions to different users. Whether for obscuring credit card numbers, social security numbers, personal patient information, or financial data, being able to encrypt specific elements in a database is becoming more important as companies increasingly share records across departments or with outside organizations.

Installing DbEncrypt 2.5.0 is relatively easy. You install a client on your workstation, then connect to the database through the client to install the server-side objects that perform the encryption. The encryption mechanisms offered by DbEncrypt are very powerful; it has 11 encryption algorithms including AES (Advanced Encryption Standard), RC4, DES, and RSA encryption. DbEncrypt also comes with code samples for all 11 encryption types, as well as sign/verify, hash, and encode/decode, to add encryption directly to your applications.

The audit trail feature allows authorized users to view information about encryption and decryption activity in the database as well as all administrative activities. The audit log may be viewed only through the DbEncrypt client utility and won’t mesh with an enterprise-level auditing solution — it audits only activity in DbEncrypt.

DbEncrypt also manages its own security. By mapping database log-ins directly to DbEncrypt log-ins, administrators can define who can and can’t use encryption and view encrypted data, all the way down to the column level. Defining encryption schemes and assigning permissions for a column or for an entire table couldn’t be easier.

Although log-ins are mapped to encryption mechanisms in DbEncrypt, they don’t give the user automatic access to the data; a separate password must also be used to log in to DbEncrypt. The unfortunate side effect of having a separate password is not only do your users have to remember two passwords just to log in to the database, it also opens up another hole on your server that’s susceptible to brute-force attacks.

One caveat with this program is its extremely invasive nature. The invasiveness can’t really be avoided, because the only way to get the kind of security that DbEncrypt offers is to permeate code throughout the database.

Here’s what it does: DbEncrypt has a series of .dlls on the server that it uses to control the encryption and user access to the encrypted columns. But to accomplish the level of security desired, it must rename the base table and create two views. The highest-level view is given the same name as the original table. This could potentially cause a huge problem because, although views are updatable, DbEncrypt requires you to remove any constraints or indexes on the columns before encrypting. This extra step could affect performance and possibly the integrity of your database.

DbEncrypt is a powerful encryption tool that allows administrators to easily secure sensitive data. However, when Microsoft SQL Server 2005 is released next year, it will make DbEncrypt unnecessary for Microsoft shops. SQL Server 2005 promises built-in encryption that will be fairly accessible to admins with just a few lines of code. — S.M.

---

**DbEncrypt 2.5.0**  
Application Security appsecinc.com  

<table>
<thead>
<tr>
<th>VERY GOOD</th>
<th>7.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manageability (25%)</td>
<td>8</td>
</tr>
<tr>
<td>Ease of Use (20%)</td>
<td>7</td>
</tr>
<tr>
<td>Performance (20%)</td>
<td>6</td>
</tr>
<tr>
<td>Reliability (15%)</td>
<td>8</td>
</tr>
<tr>
<td>Setup (10%)</td>
<td>7</td>
</tr>
<tr>
<td>Value (10%)</td>
<td>7</td>
</tr>
</tbody>
</table>

**COST:** $15,000 per Oracle SID or SQL Server Instance  
**PLATFORM:** Oracle database server, Microsoft SQL Server  
**BOTTOM LINE:** DbEncrypt is an enterprise-level database encryption utility that is easy to install and configure, and it works at the column level. Decryption of the columns can be configured through the user interface, and it is easy to add and remove permissions. However, such software will be obsolete for Microsoft shops when SQL Server 2005 is released.
Application for Free Subscription

Please answer the questions on the following page.

I WISH TO RECEIVE A FREE SUBSCRIPTION TO InfoWorld

[ ] 1. Yes  [ ] 0. No

SIGNATURE

DATE

A  MAILING ADDRESS

Publisher reserves the right to limit the number of complimentary subscriptions.
Free subscriptions available in the U.S. (including APO and FPO) and Canada.

NAME

TITLE

COMPANY NAME

DIVISION / DEPT / MAIL STOP

MAILING ADDRESS

CITY / STATE / ZIP / POSTAL CODE

BUSINESS PHONE (INCLUDING AREA CODE)

FAX NO. (INCLUDING AREA CODE)

E-MAIL ADDRESS

Is the above address a home address?

[ ] 1. Yes  [ ] 0. No

B  SPECIAL REQUEST:

You may receive a renewal reminder via e-mail. May we send other information about InfoWorld products or services via e-mail?

[ ] 1. Yes  [ ] 0. No

Reader feedback is important to us. May a member of our editorial team contact you?

[ ] 1. Yes  [ ] 0. No

WHAT IS YOUR ORGANIZATION’S PRIMARY BUSINESS ACTIVITY AT THIS LOCATION? (PLEASE CHECK ONLY ONE):

General Business Industries

[ ] 01. Defense Contractor / Aerospace
[ ] 02. Retail
[ ] 03. Wholesale / Distribution (non-computer)
[ ] 04. Pharmaceutical / Medical / Dental / Healthcare
[ ] 05. Financial Services / Banking
[ ] 06. Insurance / Real Estate / Legal
[ ] 07. Transportation / Utilities
[ ] 08. Media (print / electronic)
[ ] 09. Communication Carriers (telecomm, data comm., TV / cable)
[ ] 10. Construction / Architecture / Engineering
[ ] 11. Manufacturing & Process Industries (other than computer-related)
[ ] 12. Research / Development

Technology Providers

[ ] 13. Managed Service Provider / Business Service Provider
[ ] 14. Technology Service Provider (ISP / ASP / MSP, etc.)
[ ] 15. Computer / Network Consultant
[ ] 16. Systems or Network Integrator
[ ] 17. VAR / VAD
[ ] 18. Technology Manufacturer (hardware, software, peripherals, etc.)
[ ] 19. Technology - Related Retailer / Wholesaler / Distributor

Government / Education

[ ] 20. Government: federal (including military)
[ ] 21. Government: state or local
[ ] 22. Education

[ ] 98. Other  (Please specify)

WHAT IS YOUR PRIMARY JOB TITLE? (PLEASE CHECK ONLY ONE):

IT / Technology Professionals

[ ] 01. Chief Technology Officer (CTO)
[ ] 02. Chief Information Officer (CIO)
[ ] 03. Chief Security Officer (CSO)
[ ] 04. Vice President (including EVP, EVP, etc.)
[ ] 05. Director
[ ] 06. Manager / Supervisor
[ ] 07. Engineer
[ ] 08. Systems Analyst / Programmer / Architect
[ ] 09. Consultant / Integrator
[ ] 10. Developer
[ ] 11. IT Staff
[ ] 12. Other IT Professional  (Please specify)

Corporate / Business Management

[ ] 13. CEO, COO, President, Owner
[ ] 14. CFO, Controller, Treasurer
[ ] 15. Vice President (including EVP, EVP, etc.)
[ ] 16. Director
[ ] 17. Manager / Supervisor
[ ] 18. Other Business Management Title  (Please specify)

[ ] 98. Other Title  (Please specify)

PLEASE INDICATE YOUR JOB FUNCTION(S)?

(PLEASE CHECK ALL THAT APPLY):

IT / Technology Functions

[ ] 01. Executive
[ ] 02. Department Management - IT
[ ] 03. Research and Development Management
[ ] 04. Systems / Network Management
[ ] 05. Management of Enterprise Applications (CRM, ERP, SOM, etc.)
[ ] 06. Applications Development
[ ] 07. Consultant / Integrator
[ ] 08. Other IT Department Management

(Please describe)

[ ] 09. Other IT - Staff

(Please describe)

Corporate / Business Functions

[ ] 10. Executive
[ ] 11. Department Management - Business
[ ] 12. Financial / Accounting Management
[ ] 13. Research and Development Management
[ ] 14. Sales / Marketing Management
[ ] 15. Other Department Management
[ ] 16. Other Department Staff

(Please describe)

(Please describe)

HOW MANY PEOPLE ARE EMPLOYED AT THIS ORGANIZATION, INCLUDING ALL OF ITS BRANCHES, DIVISIONS AND SUBSIDIARIES? (PLEASE CHECK ONE ONLY):

[ ] 01. 20,000 or more
[ ] 02. 10,000 - 19,999
[ ] 03. 5,000 - 9,999
[ ] 04. 1,000 - 4,999

[ ] 05. 500 - 999
[ ] 06. 100 - 499
[ ] 07. 50 - 99
[ ] 08. Less than 49

OVER THE COURSE OF ONE YEAR, DO YOU BUY, SPECIFY, RECOMMEND, OR APPROVE THE PURCHASE OF THE FOLLOWING PRODUCTS OR SERVICES WORTH:

* CONSULTANTS: PLEASE INCLUDE WHAT YOU RECOMMEND FOR YOUR CLIENTS AS WELL AS WHAT YOU BUY FOR YOUR OWN BUSINESS, IF APPLICABLE. IF YOU CANNOT DISTINGUISH BETWEEN THIS AND OTHER LOCATIONS, PUT RESPONSE IN THE FIRST COLUMN.

01. $100 million or more
02. $50,000,000 to $99,999,999
03. $30,000,000 to $49,999,999
04. $20,000,000 to $29,999,999
05. $10,000,000 to $19,999,999
06. $4,000,000 to $9,999,999
07. $2,500,000 to $4,999,999
08. $1,000,000 to $2,499,999
09. $500,000 to $999,999
10. $100,000 to $399,999
11. $100,000 to $399,999
12. $50,000 to $99,999
13. Less than $49,999
14. None

Product category

For this location:  (write code in box)  

For other locations:  (write code in box)  

Large systems

Client computers

Networking / Telecom (including servers)

Internet / Intranet / Extranet

Security

Storage

Peripheral equipment

Software

Service / Support

Apply online at: http://subscribe.infoworld.com

Priority Code: MT4PDF

Form: 18
PLEASE TELL US YOUR INVOLVEMENT WITH YOUR COMPANY'S STRATEGIC TECHNOLOGY INITIATIVES (PLEASE CHECK ALL THAT APPLY):

- 01. Integrate Technology with company goals
- 02. Define Architecture
- 03. Choose Technology Platforms
- 04. Develop Technology Integration Strategy
- 05. Test, pilot, implement emerging technologies
- 06. Scalability Planning
- 07. Build, Run Web Services
- 08. Internet / Network Infrastructure
- 09. Customer Relationship Management
- 10. External Partnership Management
- 11. Budgeting
- 12. Recruitment & Retention
- 13. Other__________________________
  (Please describe)
- 99. None of the above

ARE YOU INVOLVED IN BUYING, SPECIFYING, RECOMMENDING OR APPROVING THE FOLLOWING SOFTWARE?
(PLEASE CHECK ALL THAT APPLY):

- 01. Enterprise / E-Business Applications
  - 02. Customer Relationship Management (CRM / eCRM)
  - 03. Enterprise Resource Planning (ERP)
  - 04. Supply Chain / Procurement
  - 05. Business Process Management
  - 06. Business Intelligence / Data Mining
  - 07. Knowledge Management
  - 08. Portals
  - 09. Collaborative Applications / Groupware
  - 10. Project Management
  - 11. Financial / Payroll / Billing
  - 12. E-business / E-commerce
  - 14. Data Warehouse
  - 15. Manufacturing
  - 16. Asset Management / Software Distribution
  - 17. Performance / Application Management
  - 18. Streaming Media
  - 19. Other Enterprise / E-Business Applications
  - 20. Integration Software
    - 21. Web Services
    - 22. Web Services Orchestration
    - 23. Application Servers
    - 24. Enterprise Application Integration (EAI) / Middleware
    - 26. Legacy Application Integration Tools
    - 27. Other Integration Software
  - 28. Application Development
    - 29. Application Development Tools
    - 30. Application Servers
    - 31. Web services
    - 32. Java / J2EE
    - 33. XML
    - 34. .NET
    - 35. Testing Tools
    - 36. Other Application Development Software
  - 37. Application Servers
  - 38. Application Development Tools
  - 39. Application Services

ARE YOU INVOLVED IN BUYING, SPECIFYING, RECOMMENDING OR APPROVING THE FOLLOWING TECHNOLOGY SERVICES?
(PLEASE CHECK ALL THAT APPLY):

- 01. Technology Services
  - 02. Systems / Application Integration
  - 03. E-Business / Internet / Intranet / Extranet
  - 04. Application Development
  - 05. Application Hosting (ASP)
  - 06. Web Hosting
  - 07. Web Development
  - 08. Security
  - 09. Storage
  - 10. Content Delivery Networks
  - 11. Disaster Recovery / Business Continuity
  - 12. Outsourcing
  - 13. Utility Computing Services
  - 14. Telecommunications
  - 15. Call Center / IT Services
  - 16. Consulting
  - 17. Other Technology Services
  - 26. Direct Attached Storage (DAS)
  - 27. Storage Blades
  - 28. Storage Backup ( Tape, Disk, Optical, RAID)
  - 29. Removable / Portable Storage
  - 30. Disaster Recovery
  - 31. Other Storage
  - 32. Security
    - 33. Anti-Virus / Content Filtering
    - 34. Firewall
    - 35. VPN (Virtual Private Network)
    - 36. Identity Management / Authenticaton
    - 37. Intrusion Detection
    - 38. Encryption
    - 39. Other Security
  - 40. Internet / Intranet / Extranet
    - 41. Web Servers
    - 42. Web Development / Authoring Tools
    - 43. Web Performance Management / Monitoring Software
    - 44. Content Management / Document Management
    - 45. Content Delivery Networks
    - 46. Internet Software
    - 47. Other Internet / Intranet / Extranet

ARE YOU INVOLVED IN BUYING, SPECIFYING, RECOMMENDING OR APPROVING THE FOLLOWING HARDWARE?
(PLEASE CHECK ALL THAT APPLY):

- 01. Hardware
  - 02. Mainframes
  - 03. NT / Windows 2000 / .NET Servers
  - 04. Unix Servers
  - 05. Linux Servers
  - 06. Blade Servers
  - 07. PCs / Workstations
  - 08. Notebooks / Laptops
  - 09. PDAs / Handhelds / Pocket PC / Wireless Devices
  - 10. Other Hardware
  - 11. Peripherals
    - 12. Laser Printers
    - 13. Inkjet Printers
    - 14. Monitors
    - 15. Flat Panel Displays
    - 16. UPS (Uninterruptible Power Supply)
    - 17. Network Printers
    - 18. Other Peripherals

WHICH OF THE FOLLOWING OPERATING SYSTEMS ARE IN USE OR PLANNED FOR USE AT THIS LOCATION? (PLEASE CHECK ALL THAT APPLY):

- 01. Windows XP
- 02. Windows 2000
- 03. Windows NT
- 04. Windows 95/98
- 05. Windows CE
- 06. Mac OS (Macintosh)
- 07. Solaris
- 08. UNIX
  - 09. Linux
  - 10. MVS, VMS, ESA
  - 11. VM
  - 12. OS 400
  - 13. Netware
  - 14. Palm OS
  - 15. Other OS

Return this form to InfoWorld, P.O. Box 3511, Northbrook, IL 60065-3511 or FAX to (847) 291-4816.
You can also apply ONLINE at http://subscribe.infoworld.com