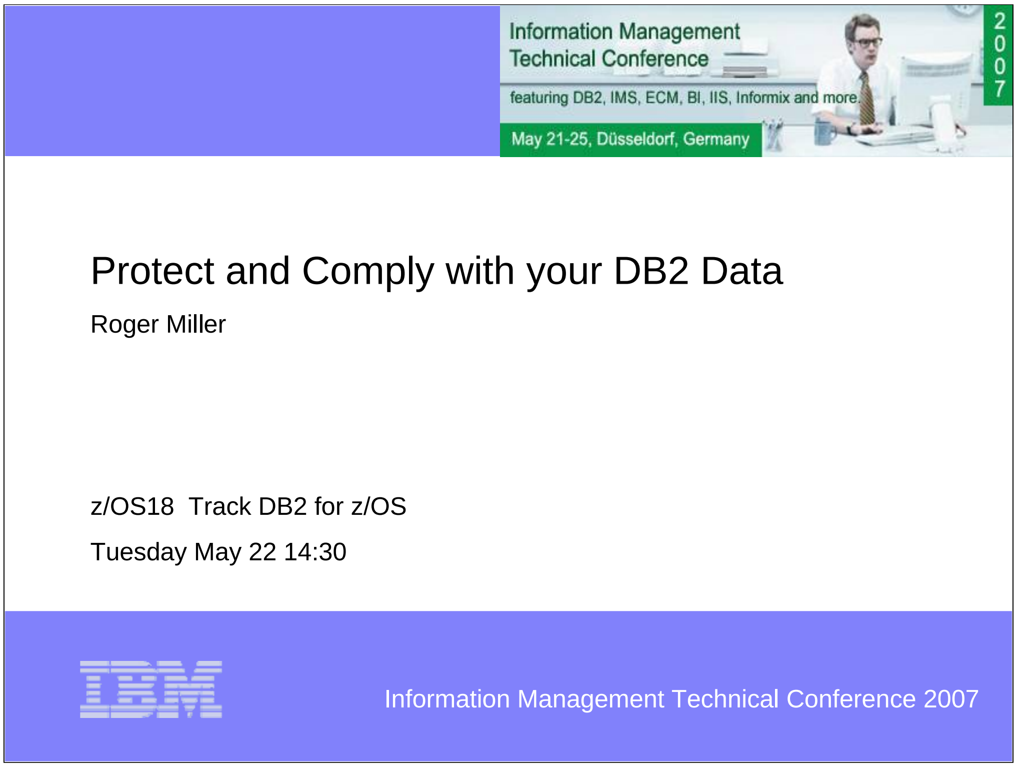


Information Management Technical Conference

featuring DB2, IMS, ECM, BI, IIS, Informix and more.

May 21-25, Düsseldorf, Germany

2007

Protect and Comply with your DB2 Data

Roger Miller

z/OS18 Track DB2 for z/OS

Tuesday May 22 14:30

Information Management Technical Conference 2007

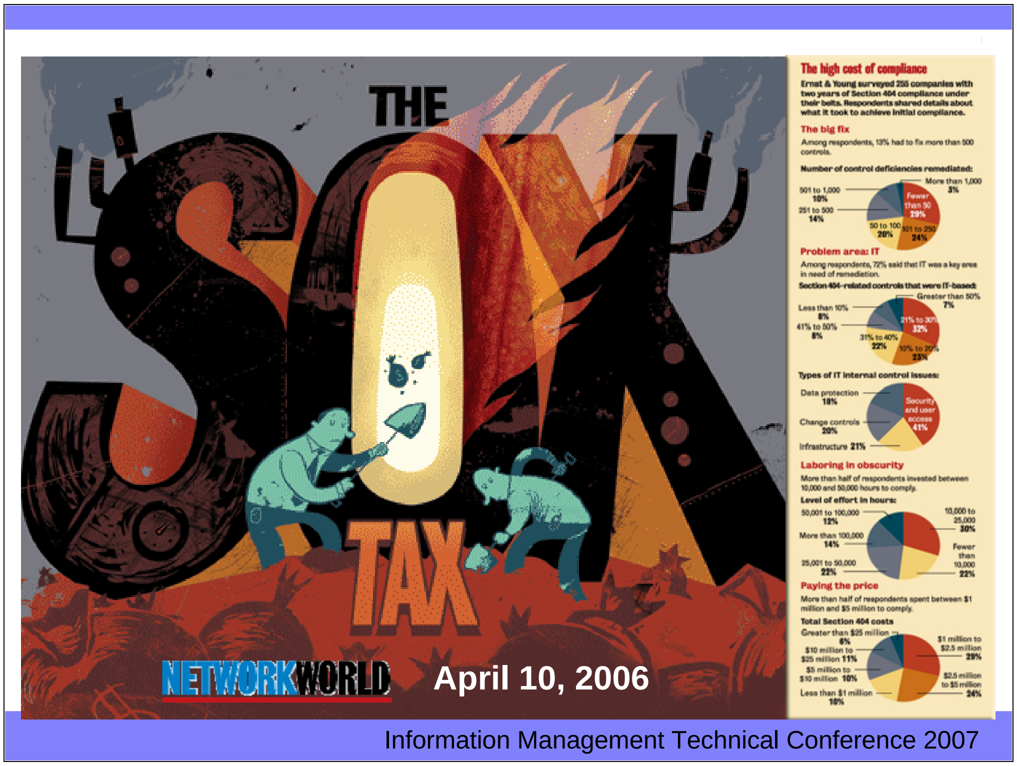
Regulatory compliance, security and audit are in the headlines and growing much more important. This session will discuss various practices for compliance and security. Encryption options for V7, V8, V9 and beyond are included. We will discuss how you can make improvements. This is a new presentation, showing how you can respond to increasing needs to protect security, integrity and comply with regulations. We'll talk about using the facilities you have and emphasize the improvements in DB2 for z/OS V8 and V9 as well as within a number of different tools.

For more details on DB2 for z/OS security, there are many suggested resources, such as the Protect Your Assets presentation:

http://www.ibm.com/support/docview.wss?rs=64&uid=swg27001877

Library for security:

http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2.doc.admin/bjndmstr124.htm



April 10, 2006

The high cost of compliance

Ernst & Young surveyed 255 companies with two years of Section 404 compliance under their belts. Respondents shared details about what it took to achieve initial compliance.

The big fix

Among respondents, 13% had to fix more than 500 controls.

Number of control deficiencies remediated:

Problem area: IT

Among respondents, 72% said that IT was a key area in need of remediation.

Section 404-related controls that were IT-based:

Types of IT internal control issues:

Laboring in obscurity

More than half of respondents invested between 10,000 and 50,000 hours to comply.

Level of effort in hours:

Paying the price

More than half of respondents spent between $1 million and $5 million to comply.

Total Section 404 costs

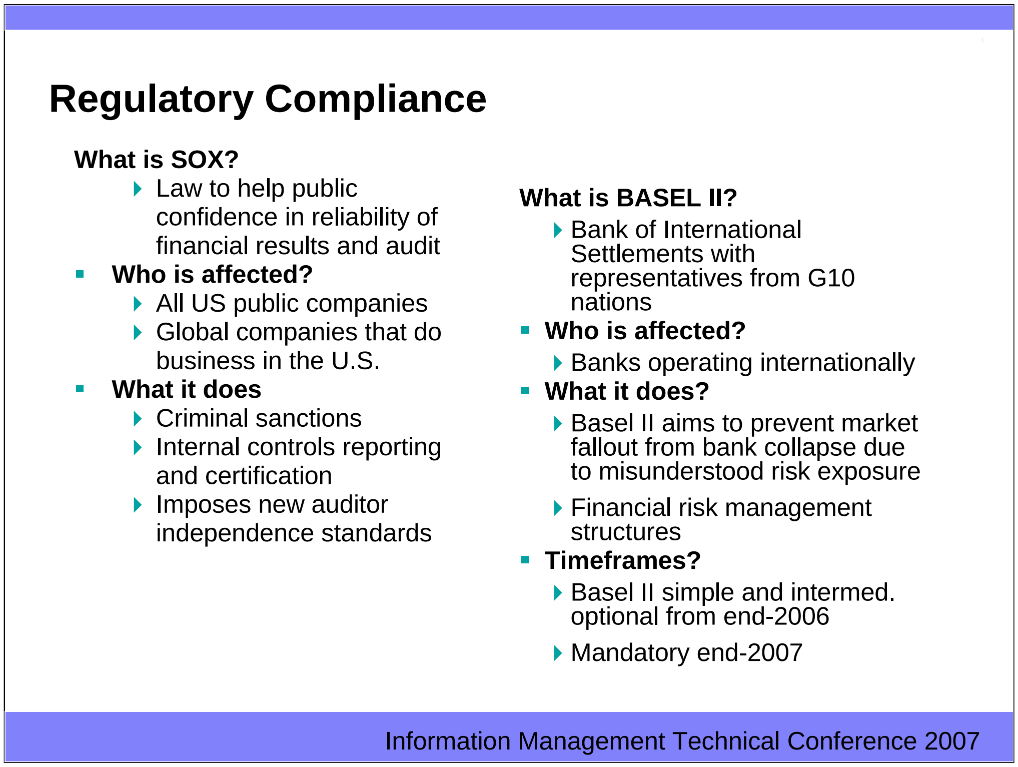
Greater than $25 million 6%
$10 million to $25 million 11%
$5 million to $10 million 10%
Less than $1 million 10%
$1 million to $2.5 million 29%
$2.5 million to $5 million 24%

Information Management Technical Conference 2007

See this article in NetWorkWorld, April 10, 2006, discussing SOX implementations. **There's a forum on the Securities and Exchange Commission Web site where a company can comment on its experiences implementing the control provisions required by Section 404 of the Sarbanes-Oxley Act. Dozens of executives have filed comments - many of which describe unreasonably onerous, expensive compliance efforts.**

"Based on our own experiences and the experiences of our peers, we believe that the effort and costs to comply with the standard have been extraordinary," said Paul Zeller, vice president and CFO of Imation in Oakdale, Minn., in a statement. "We have incurred approximately $1 million in external costs and substantially more in internal costs, such that total SOX costs approximate 5% of our 2004 operating income." …

http://www.networkworld.com/research/2006/041006-sox-tax.html



Regulatory Compliance

What is SOX?

- Law to help public confidence in reliability of financial results and audit
- **Who is affected?**
  - All US public companies
  - Global companies that do business in the U.S.
- **What it does**
  - Criminal sanctions
  - Internal controls reporting and certification
  - Imposes new auditor independence standards

What is BASEL II?

- Bank of International Settlements with representatives from G10 nations
- **Who is affected?**
  - Banks operating internationally
- **What it does?**
  - Basel II aims to prevent market fallout from bank collapse due to misunderstood risk exposure
  - Financial risk management structures
- **Timeframes?**
  - Basel II simple and intermed. optional from end-2006
  - Mandatory end-2007

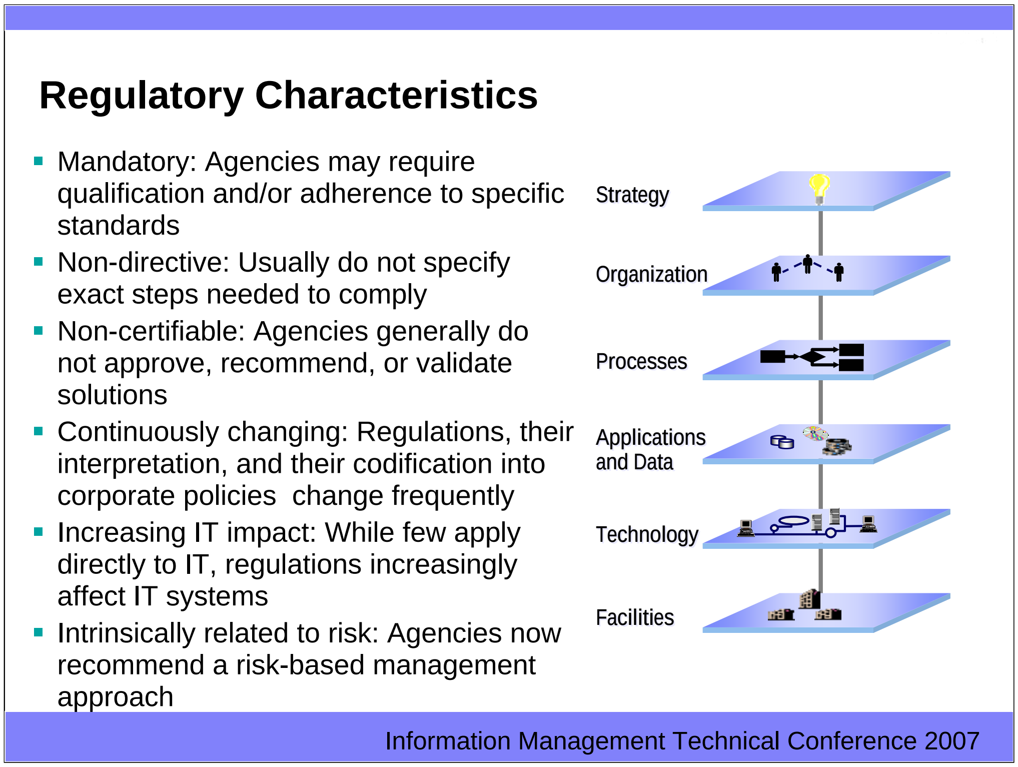
Information Management Technical Conference 2007

The explosion in government regulations and privacy acts has had a broad and profound impact on companies as a whole and the IT staff in particular. There are literally hundreds of legislative regulations and industry standards, and there are more are coming about every month. The impacts of these have been stronger in the US and Japan, but the European Union and other countries are not far behind. Two of the biggest in terms of impact are Sarbanes Oxley and Basel II. In many cases the IT department is the key to the compliance efforts.

Sarbanes Oxley was drafted by the U.S. Congress in 2002 to help increase confidence in the reliability of financial results reported by public companies. It aims to improve the accuracy of financial disclosures. The law requires global companies doing business in the US to comply and in many cases even private companies are adopting its principles. The law sets criminal sanctions for breach of certain clauses, requires reporting and certification by senior management, and imposes new auditor independence standards. Sarbanes Oxley has had a broad impact on the data center. Often compared to impact of Y2K - Sarbanes Oxley is often joked about as being Y2K on steroids; however, no one went to jail as a consequence of Y2K!

Basel II is an industry regulation directed at international financial institutions. It aims to prevent market fallout resulting from bank failures. It widely addresses risk management practices at banks, and it is meant to be applied by all financial companies whether international or not.

Both of these drive similar affects on your business: They require sound internal controls that closely relate to IT. They require assurance of secure, stable and reliable hardware and software practices. Just looking at Sarbanes Oxley again, it specifically requires that any records or transactions in the business systems of the Organization that impact assets or performance must be retained for seven (7) years. It also mandates a “record retention” system be set up and maintained. This means a centralized archiving strategy with a rock solid audit trail. It goes on to say that, if these general controls are not achieved, then the individual application controls cannot be relied upon in creating financial statements. Almost EVERY application directly or indirectly affect the financial statements. Other requirements of these regulations involve protecting and securing private data. They also require companies to be able to satisfy regulatory inspections or audits and companies must be able to trace the origins of data and processes performed against it. In other words the need for auditing information, who did what, where, and when.



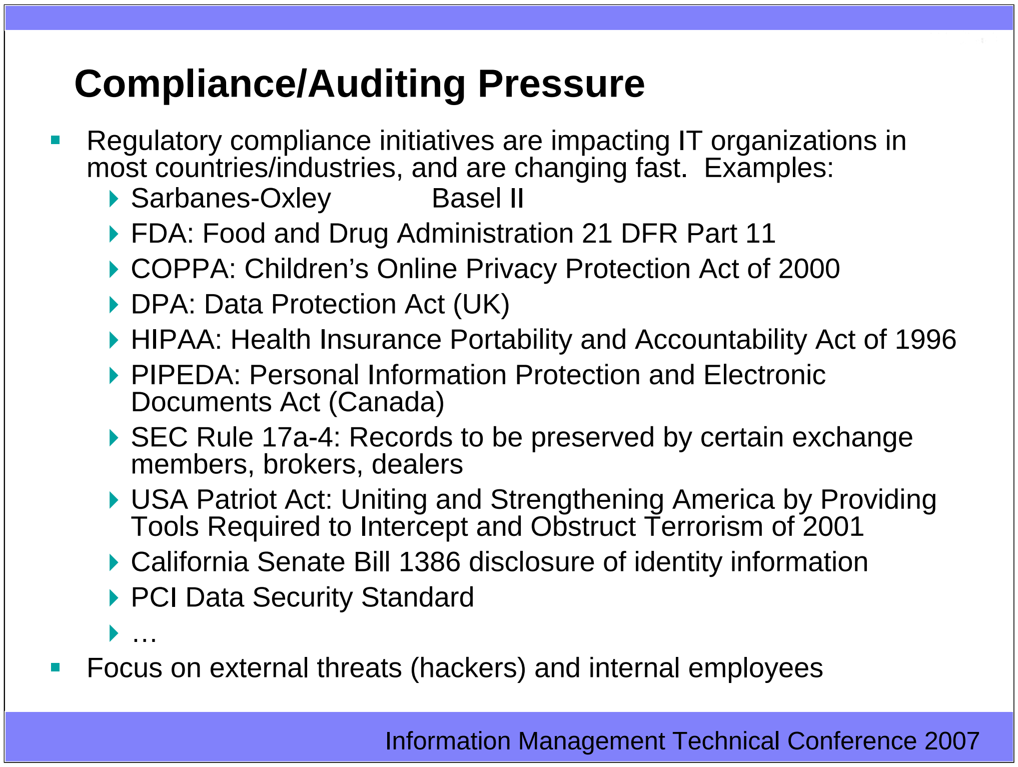
Regulatory Characteristics

- Mandatory: Agencies may require qualification and/or adherence to specific standards
- Non-directive: Usually do not specify exact steps needed to comply
- Non-certifiable: Agencies generally do not approve, recommend, or validate solutions
- Continuously changing: Regulations, their interpretation, and their codification into corporate policies change frequently
- Increasing IT impact: While few apply directly to IT, regulations increasingly affect IT systems
- Intrinsically related to risk: Agencies now recommend a risk-based management approach

Information Management Technical Conference 2007

Getting compliance with regulations is challenging. There are so many different regulations. Compliance is a condition of staying in business and out of jail. The regulations don’t specify what you need to do, so interpreting the rules is the next challenge. Since solutions are not specified, recommended or validated, these tasks are added to the compliance effort. If you are in compliance, then the regulations often change, so that a new effort is needed. Sometimes an interpretation of the regulations is changed, new regulations are added, or your business changes to make additional regulations applicable.

These regulations are having more and more impact upon information technology, and most of the impact is indirect, compliance with business rules. Compliance is related to many areas of the business: security, privacy, government relations and audit, but the essence of the work is related to risk management.



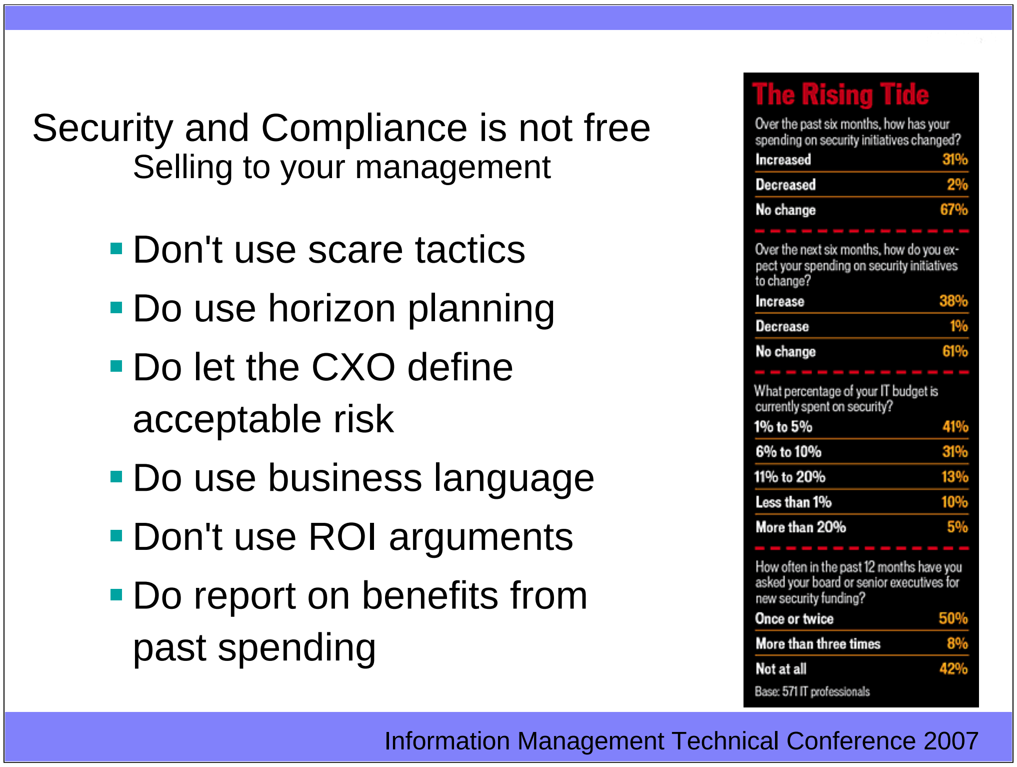
Compliance/Auditing Pressure

- Regulatory compliance initiatives are impacting IT organizations in most countries/industries, and are changing fast. Examples:
  - Sarbanes-Oxley   Basel II
  - FDA: Food and Drug Administration 21 DFR Part 11
  - COPPA: Children’s Online Privacy Protection Act of 2000
  - DPA: Data Protection Act (UK)
  - HIPAA: Health Insurance Portability and Accountability Act of 1996
  - PIPEDA: Personal Information Protection and Electronic Documents Act (Canada)
  - SEC Rule 17a-4: Records to be preserved by certain exchange members, brokers, dealers
  - USA Patriot Act: Uniting and Strengthening America by Providing Tools Required to Intercept and Obstruct Terrorism of 2001
  - California Senate Bill 1386 disclosure of identity information
  - PCI Data Security Standard
  - …
- Focus on external threats (hackers) and internal employees

Information Management Technical Conference 2007

The pressure for auditing is very different in various countries and sometimes in states, with different concerns and different laws. In general, Europe has much stronger legislation on privacy, but the world is catching up very quickly. Concern for electronic theft and identity theft has accelerated quickly and continues to climb. While the early challenges on the web were often amateurs looking for attention, the current situation is more targeted, more professional, and more criminal.

So compliance and audit have turned from a focus on just external threats and need to address employees as well. In words I heard from Donn Parker of SRI long ago, “The crooks will never catch up with the losses caused by sloppy work.”



Security and Compliance is not free

Selling to your management

- Don't use scare tactics
- Do use horizon planning
- Do let the CXO define acceptable risk
- Do use business language
- Don't use ROI arguments
- Do report on benefits from past spending

The Rising Tide

Over the past six months, how has your spending on security initiatives changed?

Increased	31%
Decreased	2%
No change	67%

Over the next six months, how do you expect your spending on security initiatives to change?

Increase	38%
Decrease	1%
No change	61%

What percentage of your IT budget is currently spent on security?

1% to 5%	41%
6% to 10%	31%
11% to 20%	13%
Less than 1%	10%
More than 20%	5%

How often in the past 12 months have you asked your board or senior executives for new security funding?

Once or twice	50%
More than three times	8%
Not at all	42%

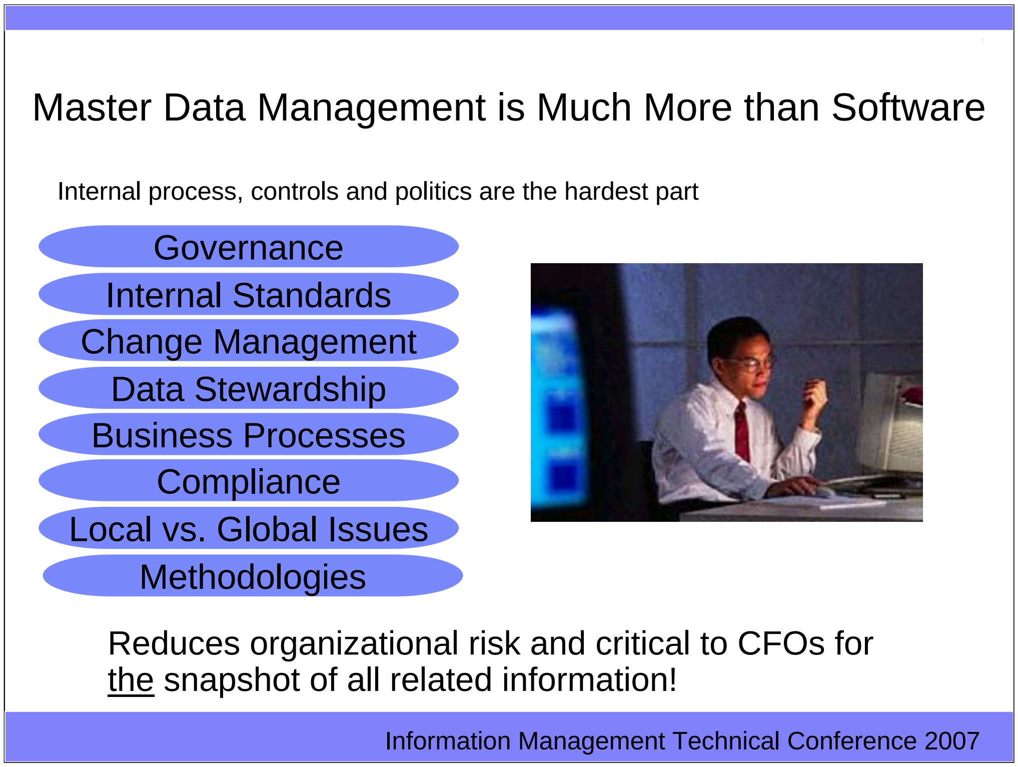
Base: 571 IT professionals

Information Management Technical Conference 2007

These articles in ComputerWorld are helpful in explaining the needs to your management. This article provides useful advice about techniques which have worked and some that have not.

http://www.computerworld.com/blogs/node/2338?NLT_SEC_B

http://www.computerworld.com/securitytopics/security/story/0,10801,110504,00.html



Master Data Management is Much More than Software

Internal process, controls and politics are the hardest part

- Governance
- Internal Standards
- Change Management
- Data Stewardship
- Business Processes
- Compliance
- Local vs. Global Issues
- Methodologies

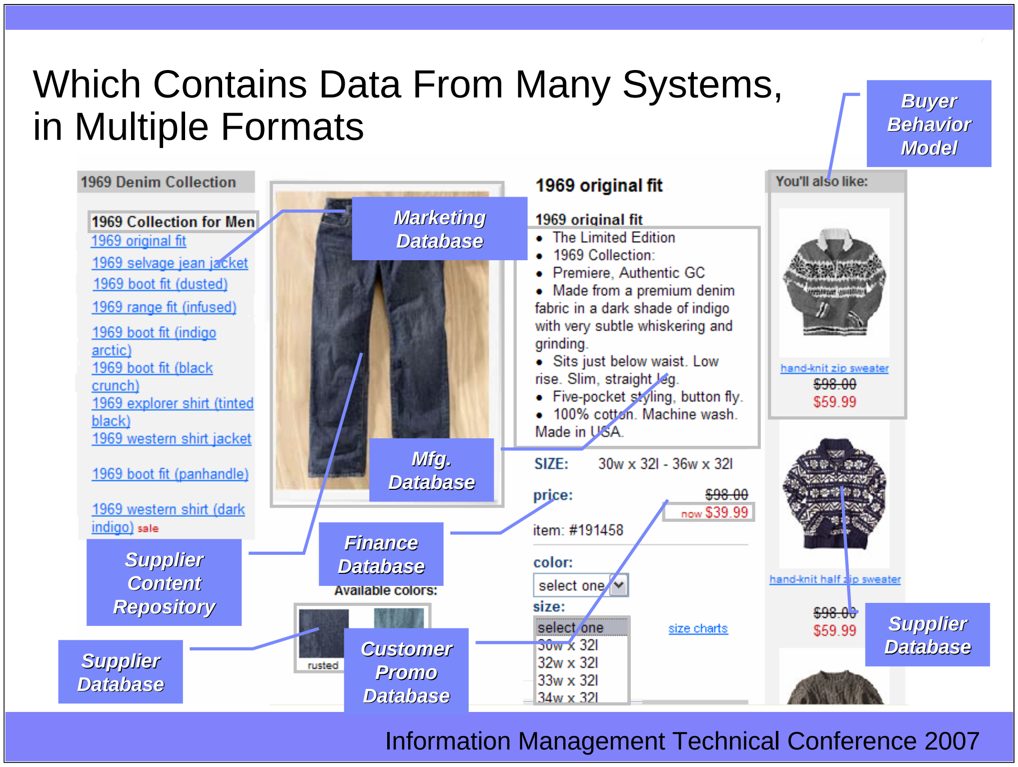
Reduces organizational risk and critical to CFOs for
the snapshot of all related information!

Information Management Technical Conference 2007

Improving controls for one version of the truth: Many issues for regulatory compliance are about improving controls. With a bewildering array of federal government, state government and industry-specific regulations and privacy acts, businesses have been driven to improve risk management, financial reporting processes and information security. The need for improvements is, in turn, driving technology investments to encrypt sensitive data, to protect sensitive data, to save data for future audits and to comply with retention rules, and auditing.

You have your mainframe protecting your data, storing it for easy access and serving it efficiently. What about the data itself? How does redundant, inaccurate or unclean data impact customer satisfaction or even compliance?

Having different sets of business data is very common because applications often function as a silo smokestack. They may share names and account numbers with other applications across an enterprise, but they run and store that data independently and just a little differently. This is one of the prime reasons that businesses want to have one set of correct customer information. Incorrect information hurts customer satisfaction. Correcting this problem is not just good for compliance. It's very good for business.



Which Contains Data From Many Systems, in Multiple Formats

1969 Denim Collection

1969 Collection for Men

1969 original fit
1969 selvage jean jacket
1969 boot fit (dusted)
1969 range fit (infused)
1969 boot fit (indigo arctic)
1969 boot fit (black crunch)
1969 explorer shirt (tinted black)
1969 western shirt jacket
1969 boot fit (panhandle)
1969 western shirt (dark indigo) sale

Available colors:

rusted

1969 original fit

1969 original fit

- The Limited Edition
- 1969 Collection:
- Premiere, Authentic GC
- Made from a premium denim fabric in a dark shade of indigo with very subtle whiskering and grinding.
- Sits just below waist. Low rise. Slim, straight leg.
- Five-pocket styling, button fly.
- 100% cotton. Machine wash. Made in USA.

SIZE: 30w x 32l - 36w x 32l

price: ~~$98.00~~ now $39.99

item: #191458

color:

select one

size:

select one
30w x 32l
32w x 32l
33w x 32l
34w x 32l

size charts

You'll also like:

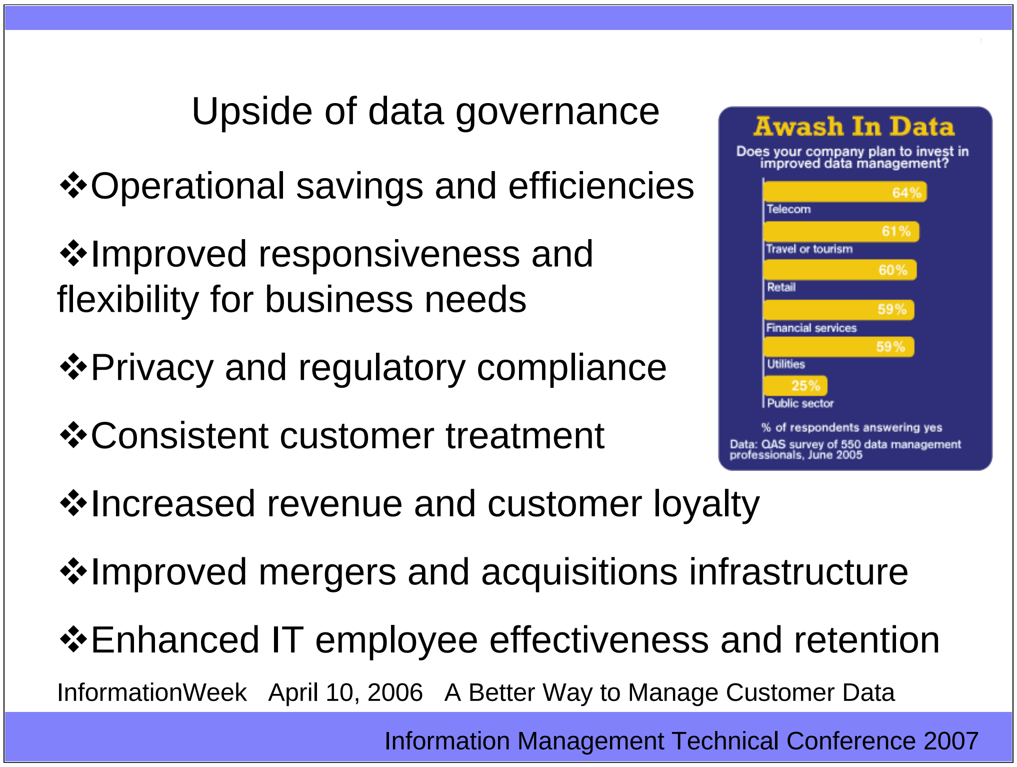
hand-knit zip sweater
~~$98.00~~
$59.99

hand-knit half zip sweater
~~$98.00~~
$59.99

Information Management Technical Conference 2007

“One version of the truth” is a complex concept that’s growing even more complex as companies are acquired, and businesses build more subsystems into their enterprises. Master data management has emerged as an important way to improve information delivery in the enterprise, enabling businesses to make better decisions by providing richer, more accurate and more contextual information. Many companies are using IBM master data management software to standardize product information used throughout their enterprise and supply chain.

But the handling of customer data remains a thorny business issue. If companies aren't struggling to determine which versions of their customer records are accurate and up to date, they're scrambling to do damage control in the wake of security breaches that expose sensitive information to prying eyes.



Upside of data governance

❖Operational savings and efficiencies

❖Improved responsiveness and flexibility for business needs

❖Privacy and regulatory compliance

❖Consistent customer treatment

❖Increased revenue and customer loyalty

❖Improved mergers and acquisitions infrastructure

❖Enhanced IT employee effectiveness and retention

InformationWeek April 10, 2006 A Better Way to Manage Customer Data

Information Management Technical Conference 2007

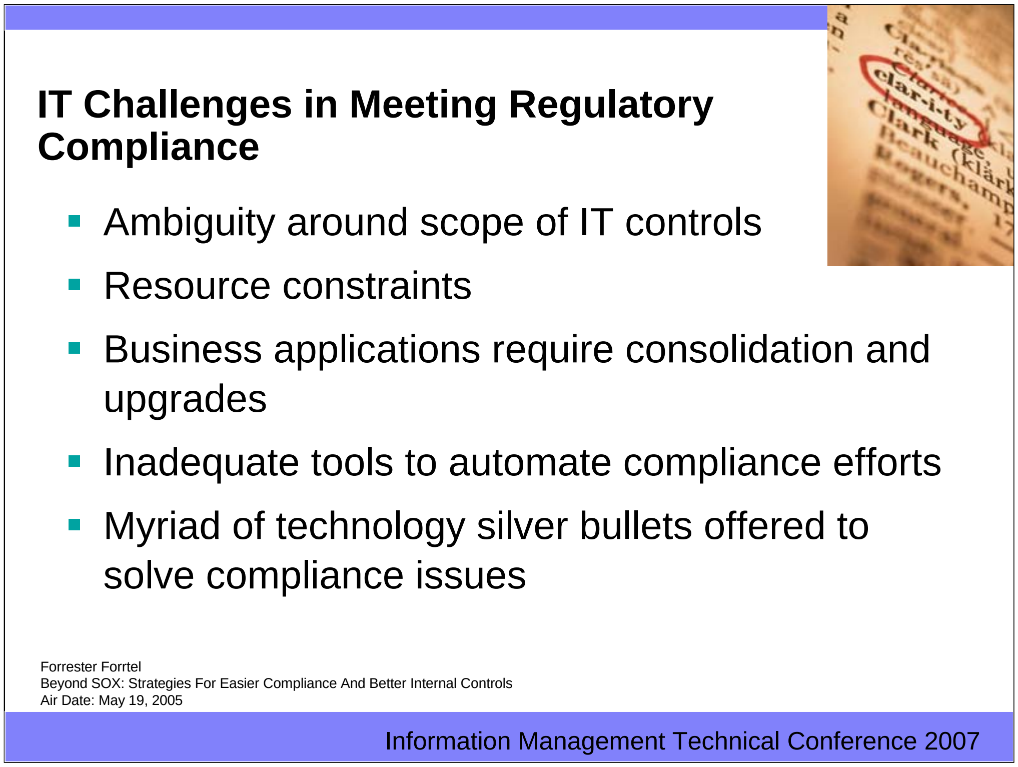
Awash In Data
Does your company plan to invest in improved data management?
64%
Telecom
61%
Travel or tourism
60%
Retail
59%
Financial services
59%
Utilities
25%
Public sector
% of respondents answering yes
Data: QAS survey of 550 data management professionals, June 2005

Another useful article in InformationWeek: Handling of customer data is one of the thorniest business issues of the 21st century. If companies aren't struggling to determine which versions of their customer records are accurate and up to date (master data management) they're scrambling to do damage control in the wake of security breaches that expose sensitive information to prying eyes (authorization, encryption and audit).

While there are countless software products designed to aid in tackling those issues, it may be the emerging business practice known as data governance that holds the most potential for companies to get a handle on their fast-growing pools of information.

Data governance is an idea that's gaining momentum among IT and security executives who are proclaiming that enough is enough. And with good reason: Companies estimate they're losing 6% of sales because of poor management of customer data, according to a recent survey conducted by data broker Experian's QAS division for data quality management.

http://www.informationweek.com/shared/printableArticle.jhtml?articleID=184429463



IT Challenges in Meeting Regulatory Compliance

- Ambiguity around scope of IT controls
- Resource constraints
- Business applications require consolidation and upgrades
- Inadequate tools to automate compliance efforts
- Myriad of technology silver bullets offered to solve compliance issues

Forrester Forrtel
Beyond SOX: Strategies For Easier Compliance And Better Internal Controls
Air Date: May 19, 2005

Information Management Technical Conference 2007

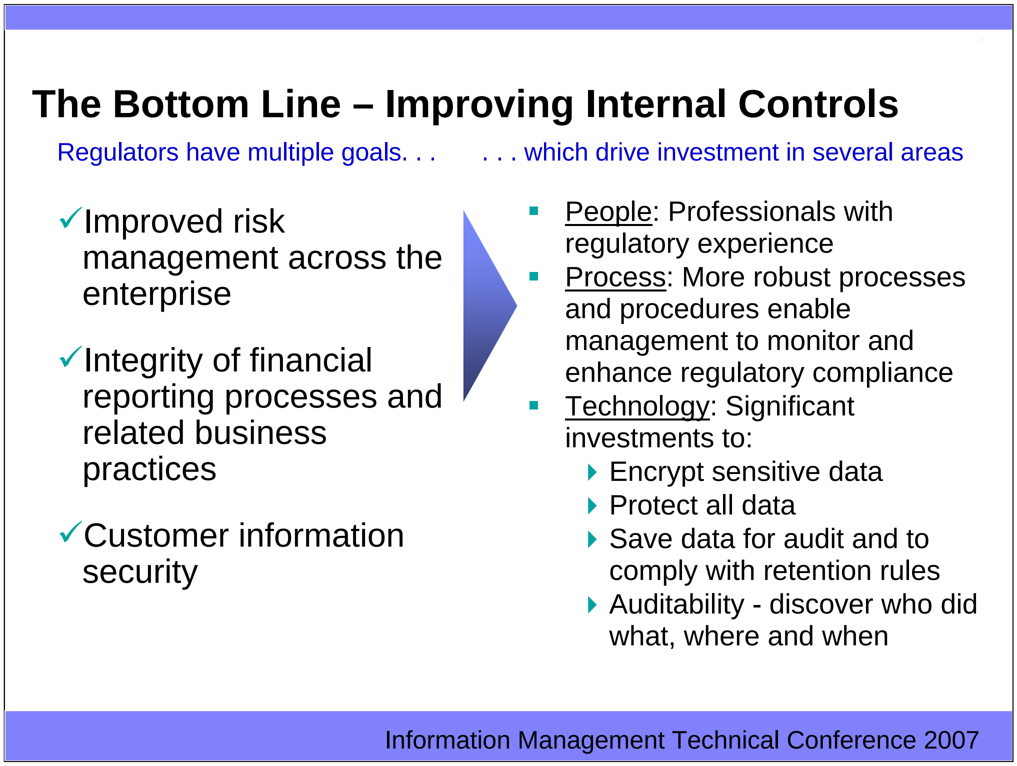
However these regulations bring upon a set of challenges that are daunting to many companies. Ambiguity around scope of IT controls: For example, Sarbanes Oxley has over 50 acts with uncountable sub-provisions. These regulations were written by accountants, auditors, and lawyers, not IT people. Many companies are struggling with how to translate these into firm requirements for their IT systems. Interestingly, although there is considerable ambiguity around these requirements, the penalties for non-compliance aren't ambiguous. They are very clear. They include fines, sanctions, lawsuits, possible imprisonment of top executives and what may be the worst of all – negative publicity for the company.

Resource constraints: It's the old do more with less. Probably not many of your budgets are growing. At the same time the ambiguity around these regulations make them difficult to know how to resource the work.

Business applications require consolidation and upgrades: If it were only the systems we had to worry about that would be one challenge. But in some cases the applications need to change as well, introducing a whole other set of challenges. One example is retention periods (archiving). If you manage your archiving on a non-uniform application-by-application basis (as many do), this could have an impact.

Inadequate tools to automate compliance efforts and Myriad of technology silver bullets offered to solve compliance issues. Vendors will try and sell you a single 'silver bullet' tools offering to solve all of your compliance issues. Don't believe it! The real world is more complex than this and reality says that you will need to work carefully to set up a strong, comprehensive set of policies (internal controls) to achieve compliance. A variety of tools and processes will assist you in doing this.

You've got to consider the OLTP systems (operational data), financial data, your content data (unstructured data), spreadsheets, e-mail, and business intelligence data. IBM and other vendors provide a number of tools to help in all aspects of this problem.



The Bottom Line – Improving Internal Controls

Regulators have multiple goals. . .

. . . which drive investment in several areas

✓Improved risk management across the enterprise

✓Integrity of financial reporting processes and related business practices

✓Customer information security

- People: Professionals with regulatory experience
- Process: More robust processes and procedures enable management to monitor and enhance regulatory compliance
- Technology: Significant investments to:
  - Encrypt sensitive data
  - Protect all data
  - Save data for audit and to comply with retention rules
  - Auditability - discover who did what, where and when

Information Management Technical Conference 2007

So in summary, we have a bewildering array of federal government, state government, and industry specific regulations and privacy acts. This is driving businesses to improve:

Risk management across the enterprise and to solidify internal controls

Financial reporting processes and secure business practices

Protecting information security – privacy data and system access

… and this is driving investment in several areas

People, internal auditors and external auditors are becoming more pervasive, especially in industries like finance and insurance.

Stricter processes which allow top management to monitor regulatory compliance

Technology, the need to invest in tools to help you achieve these goals:

Encrypt sensitive data

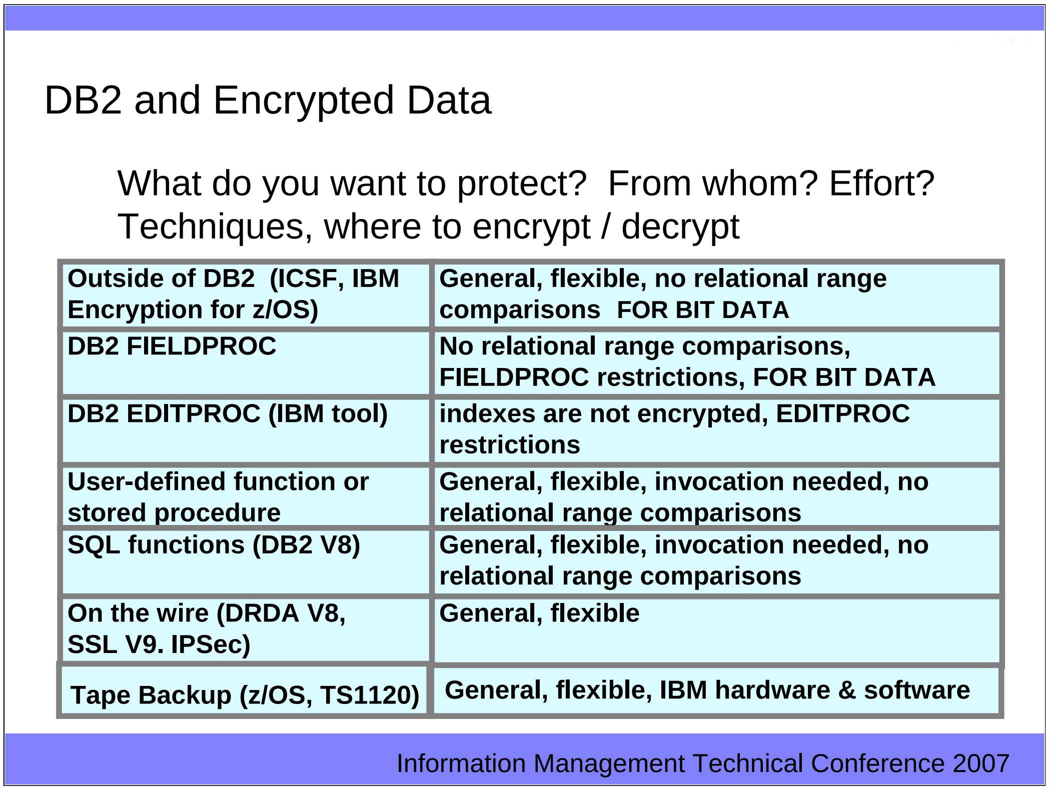
Protect sensitive production data

Save data for future audits and to comply with retention rules

Auditability - discover who did what, where and when

Real time

Historically

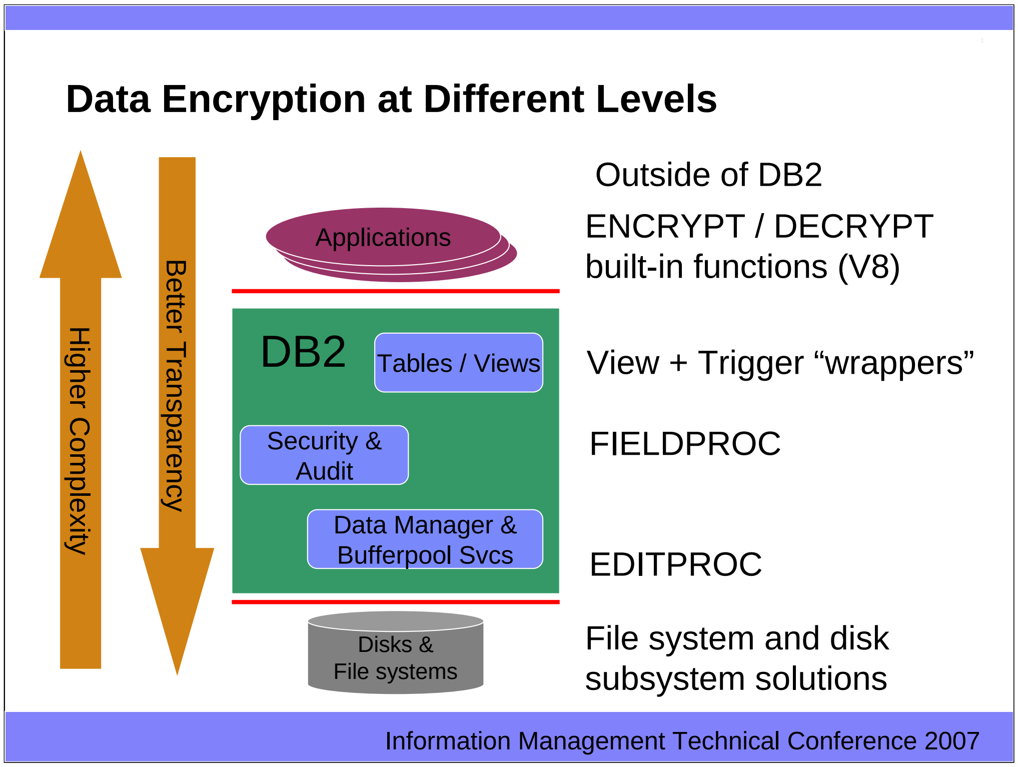


DB2 and Encrypted Data

What do you want to protect? From whom? Effort?
Techniques, where to encrypt / decrypt

Outside of DB2 (ICSF, IBM Encryption for z/OS)	**General, flexible, no relational range comparisons FOR BIT DATA**
DB2 FIELDPROC	**No relational range comparisons, FIELDPROC restrictions, FOR BIT DATA**
DB2 EDITPROC (IBM tool)	**indexes are not encrypted, EDITPROC restrictions**
User-defined function or stored procedure	**General, flexible, invocation needed, no relational range comparisons**
SQL functions (DB2 V8)	**General, flexible, invocation needed, no relational range comparisons**
On the wire (DRDA V8, SSL V9. IPSec)	**General, flexible**
Tape Backup (z/OS, TS1120)	**General, flexible, IBM hardware & software**

There are many ways to encrypt data in DB2. The answers to the questions, "What do you want to protect and from whom?" and “How much effort can be used?” are generally needed to determine which technique to use and where to encrypt and decrypt. Encryption does mean some tradeoffs in function, usability and performance. Either the indexes are not encrypted or encrypted data will not give correct results for comparisons other than equals or not equals. All greater than, less than and range predicates are not usable. An EDITPROC is the most used technique, and one is provided to use cryptography hardware with an IBM Tool. The CMOS Cryptographic Coprocessors feature and ICRF hardware were designed to address high volume cryptographic transaction rates and bulk security requirements on z/OS. The Integrated Cryptographic Service Facility (ICSF) and the IBM Encryption Facility for z/OS provide the interfaces to service routines supported by the hardware, such as key management.
http://www.ibm.com/servers/eserver/zseries/security/cryptography.html



Data Encryption at Different Levels

Outside of DB2

ENCRYPT / DECRYPT
built-in functions (V8)

View + Trigger “wrappers”

FIELDPROC

EDITPROC

File system and disk
subsystem solutions

Information Management Technical Conference 2007

This diagram shows the range of places where data encryption can be performed. It is complementary to the prior page, which indicates some of the specific challenges.

If the applications are already written, then there is generally a very high need for transparency. But transparency means that some kinds of protection are not provided.

Some vendors address encryption as well.

Here are the primary references for encryption in DB2.

http://www.ibm.com/developerworks/db2/library/techarticle/benfield/0108benfield.html

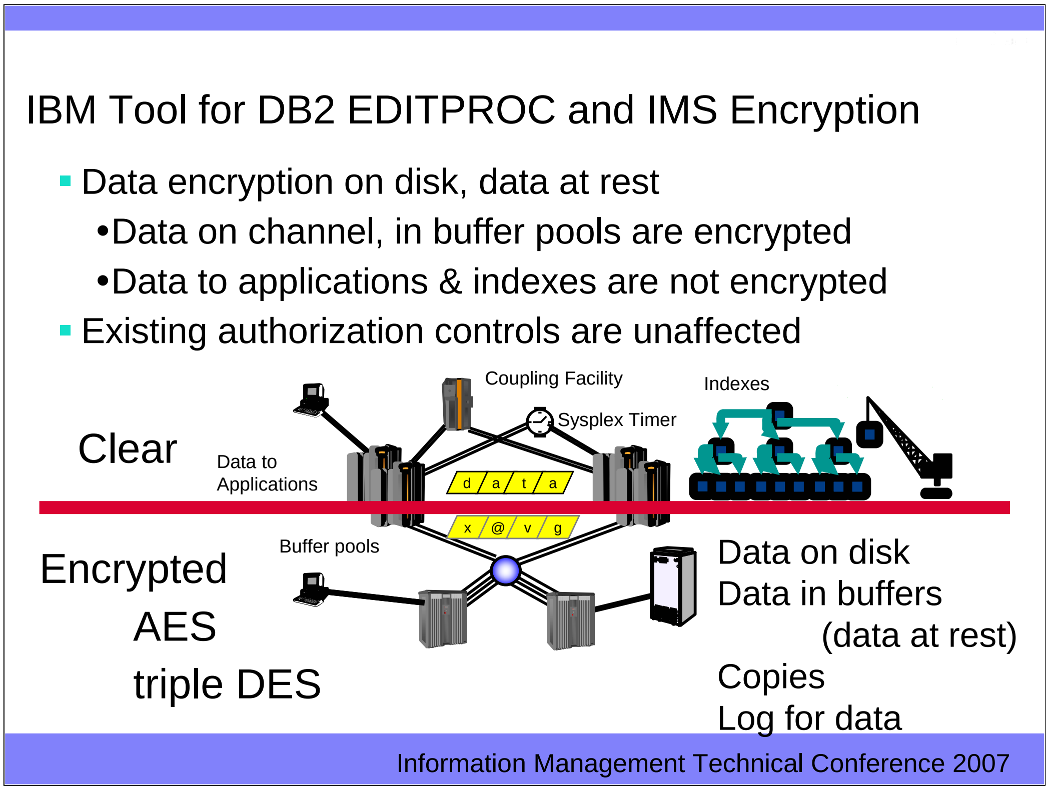
http://www.ibm.com/support/docview.wss?uid=swg21168217

http://www.ibm.com/support/docview.wss?uid=swg27007844&aid=1

http://www.ibm.com/support/docview.wss?uid=swg27007842&aid=1

http://www.redbooks.ibm.com/redbooks/pdfs/sg247111.pdf

sections 1.1.13 & 1.1.14



IBM Tool for DB2 EDITPROC and IMS Encryption

- Data encryption on disk, data at rest
  - •Data on channel, in buffer pools are encrypted
  - •Data to applications & indexes are not encrypted
- Existing authorization controls are unaffected

Clear

Encrypted

AES

triple DES

Data on disk
Data in buffers
(data at rest)
Copies
Log for data

Information Management Technical Conference 2007

On this slide, data above the middle line is not encrypted and data below the line is encrypted.

In this example, the encryption is not providing an additional level of security for your DB2 or IMS applications. It is providing encryption of the data on the disk.

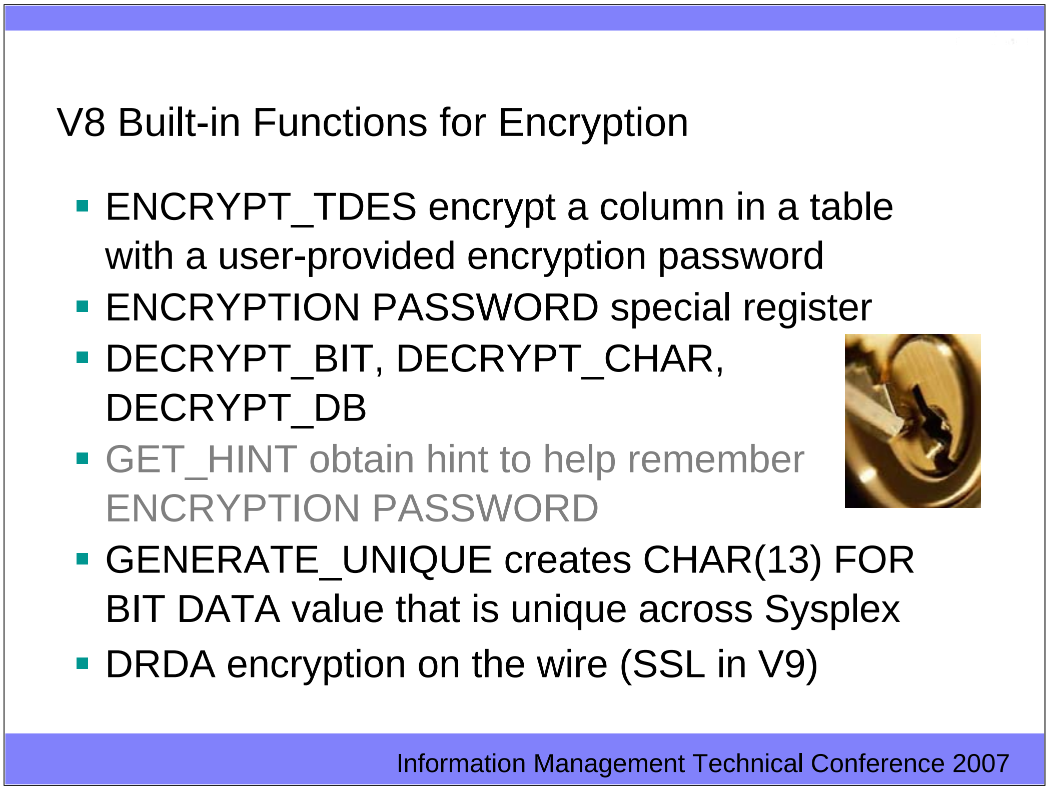
Once the data is brought, for example, into DBMS working storage, you are using the existing DB2 and IMS authorizations to secure data. As the data is written out to disk, that is once it leaves the channel and enters the network to move to the disk, the data is encrypted.

The example on this slide shows two subsystems with disks. The circle on the bottom half of the picture might be what we have known as an ESCON director in the past. The processor on the right hand side, below the line, might also be attached to that same I/O device; however, if the processor is a zSeries system that does not have the encryption key it will not be able to interpret the data.

See the DB2 tools web pages for more about this.

http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html

http://www.ibm.com/software/os/zseries/telecon/14sep/



V8 Built-in Functions for Encryption

- ENCRYPT_TDES encrypt a column in a table with a user-provided encryption password
- ENCRYPTION PASSWORD special register
- DECRYPT_BIT, DECRYPT_CHAR, DECRYPT_DB
- GET_HINT obtain hint to help remember ENCRYPTION PASSWORD
- GENERATE_UNIQUE creates CHAR(13) FOR BIT DATA value that is unique across Sysplex
- DRDA encryption on the wire (SSL in V9)

Information Management Technical Conference 2007

If you want to have very flexible encryption and decryption in your applications, then functions ENCRYPT_TDES (triple DES), DECRYPT_BIN, DECRYPT_CHAR, and GETHINT are added. The SET ENCRYPTION PASSWORD statement allows the application to specify a password
The ability to generate a unique value is also included. These changes came in DB2 for Linux, UNIX and Windows V8, so this change improves DB2 family consistency.
The difficult part of encryption and decryption is key management, which becomes the responsibility of the applications, if they perform the encryption.

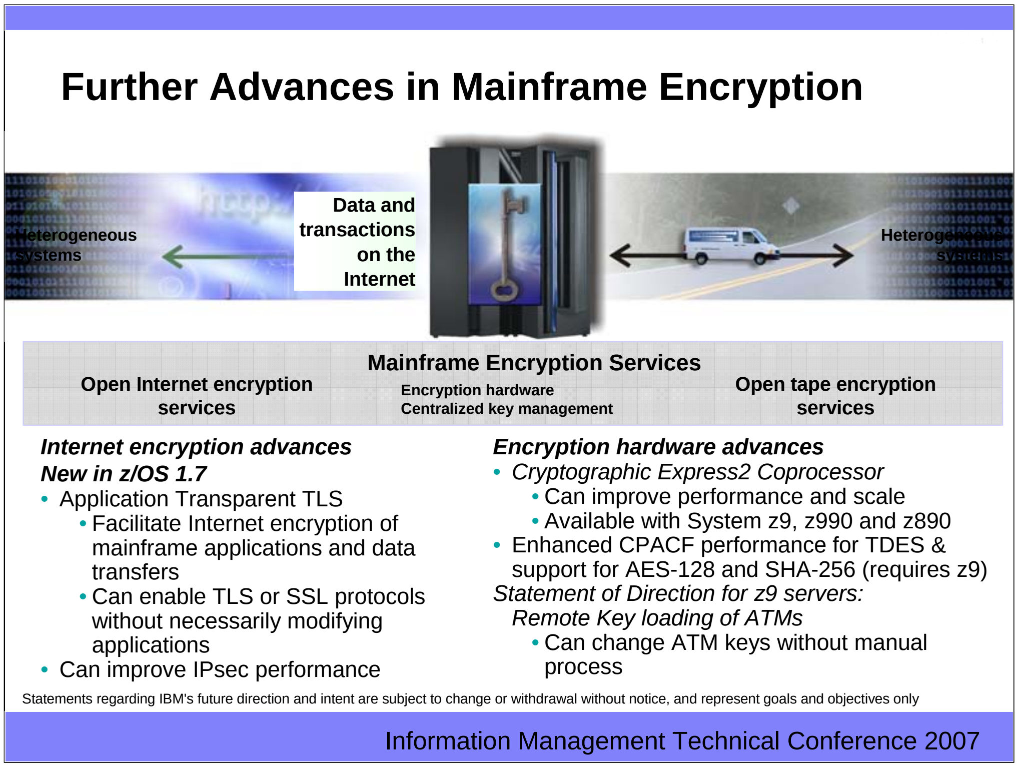
DRDA is extended to allow encryption of the data being sent. The DB2 Connect change is provided in V8.2 or fixpak 7A or later. Fixpak 10 is the recommended level.

Here are the primary references for encryption in DB2.

http://www.ibm.com/developerworks/db2/library/techarticle/benfield/0108benfield.html

http://www.ibm.com/support/docview.wss?uid=swg21168217

http://www.redbooks.ibm.com/redbooks/pdfs/sg247111.pdf sections 1.1.13 & 1.1.14


Heterogeneous systems
Data and transactions on the Internet
Heterogeneous systems

Further Advances in Mainframe Encryption

Mainframe Encryption Services

Open Internet encryption services

Encryption hardware
Centralized key management

Open tape encryption services

Internet encryption advances
New in z/OS 1.7

- Application Transparent TLS
  - Facilitate Internet encryption of mainframe applications and data transfers
  - Can enable TLS or SSL protocols without necessarily modifying applications
- Can improve IPsec performance

Encryption hardware advances

- *Cryptographic Express2 Coprocessor*
  - Can improve performance and scale
  - Available with System z9, z990 and z890
- Enhanced CPACF performance for TDES & support for AES-128 and SHA-256 (requires z9)

Statement of Direction for z9 servers:
Remote Key loading of ATMs

- Can change ATM keys without manual process

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only

Information Management Technical Conference 2007

Improvements in encryption come in our new processors and in new operating system releases, as well as in new releases of software.

Application Transparent TLS

Facilitate Internet encryption of mainframe applications and data transfers

Can enable TLS or SSL protocols without necessarily modifying applications

Can improve IPsec performance

Cryptographic Express2 Coprocessor

Can improve performance and scale

Available with System z9, z990 and z890

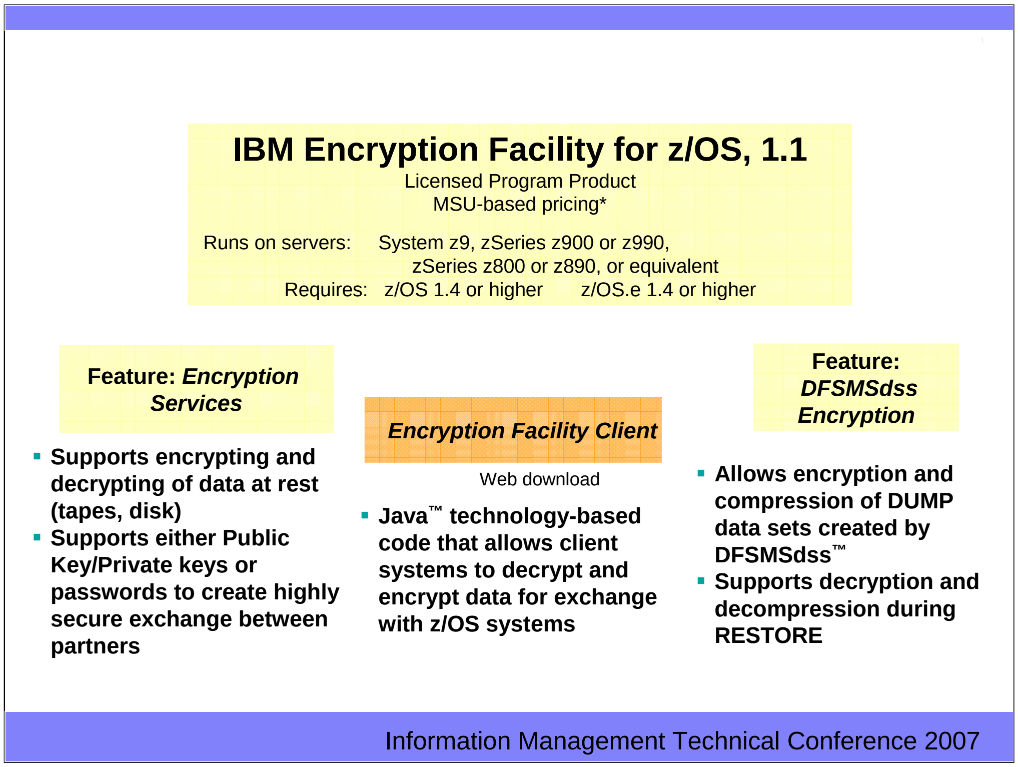
Enhanced CPACF performance for TDES & support for AES-128 and SHA-256 (requires z9)

Statement of Direction for z9 servers:

Remote Key loading of ATMs

Can change ATM keys without manual process

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only



IBM Encryption Facility for z/OS, 1.1

Licensed Program Product
MSU-based pricing*

Runs on servers: System z9, zSeries z900 or z990,
zSeries z800 or z890, or equivalent
Requires: z/OS 1.4 or higher z/OS.e 1.4 or higher

Feature: *Encryption Services*

- **Supports encrypting and decrypting of data at rest (tapes, disk)**
- **Supports either Public Key/Private keys or passwords to create highly secure exchange between partners**

Encryption Facility Client

Web download

- **Java™ technology-based code that allows client systems to decrypt and encrypt data for exchange with z/OS systems**

Feature: *DFSMSdss Encryption*

- **Allows encryption and compression of DUMP data sets created by DFSMSdss™**
- **Supports decryption and decompression during RESTORE**

Information Management Technical Conference 2007

The Encryption Services feature supports encrypting and decrypting of data at rest (tapes, disk) and supports either Public Key/Private keys or passwords to create highly secure exchange between partners.

The Encryption Facility Client is Java™ technology-based code that allows client systems to decrypt and encrypt data for exchange with z/OS systems.

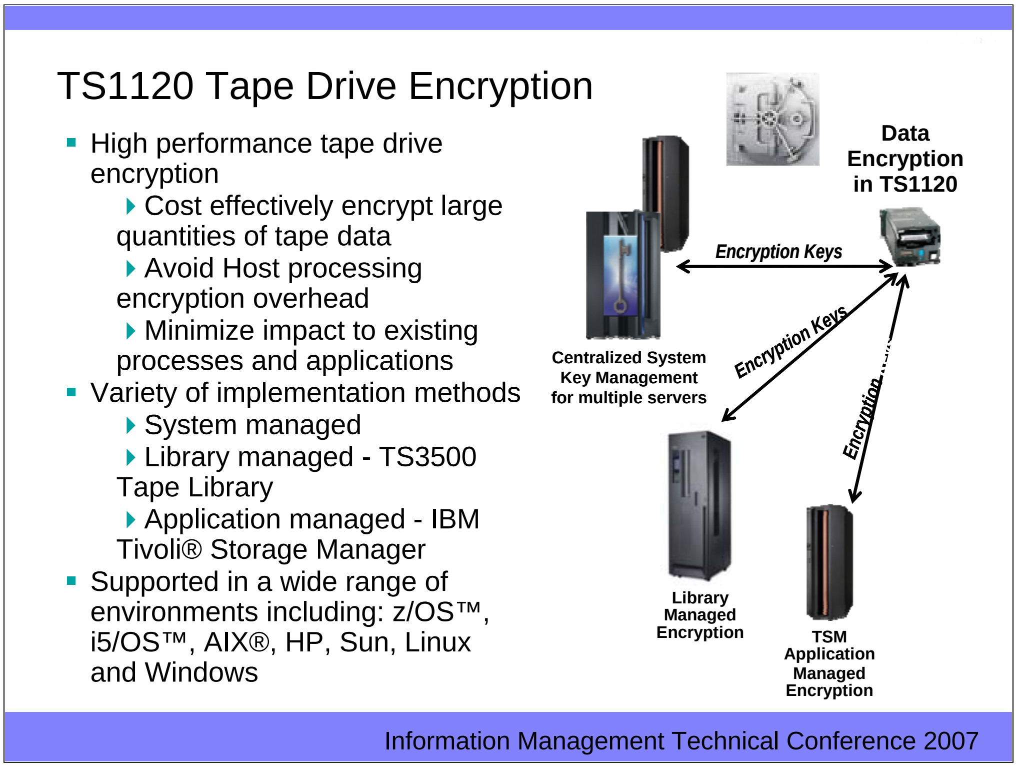
The DFSMSdss Encryption feature allows encryption and compression of DUMP data sets created by DFSMSdss™. It supports decryption and decompression during RESTORE.

•Variable Workload License Charges (VWLC), Entry Workload License Charges (EWLC), zSeries Entry License Charges™ (zELC), Parallel Sysplex License Charges (PSLC)

http://www.ibm.com/systems/systemz9/feature092705/

http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/

http://www.ibm.com/common/ssi/rep_ca/3/897/ENUS205-243/ENUS205-243.PDF



TS1120 Tape Drive Encryption

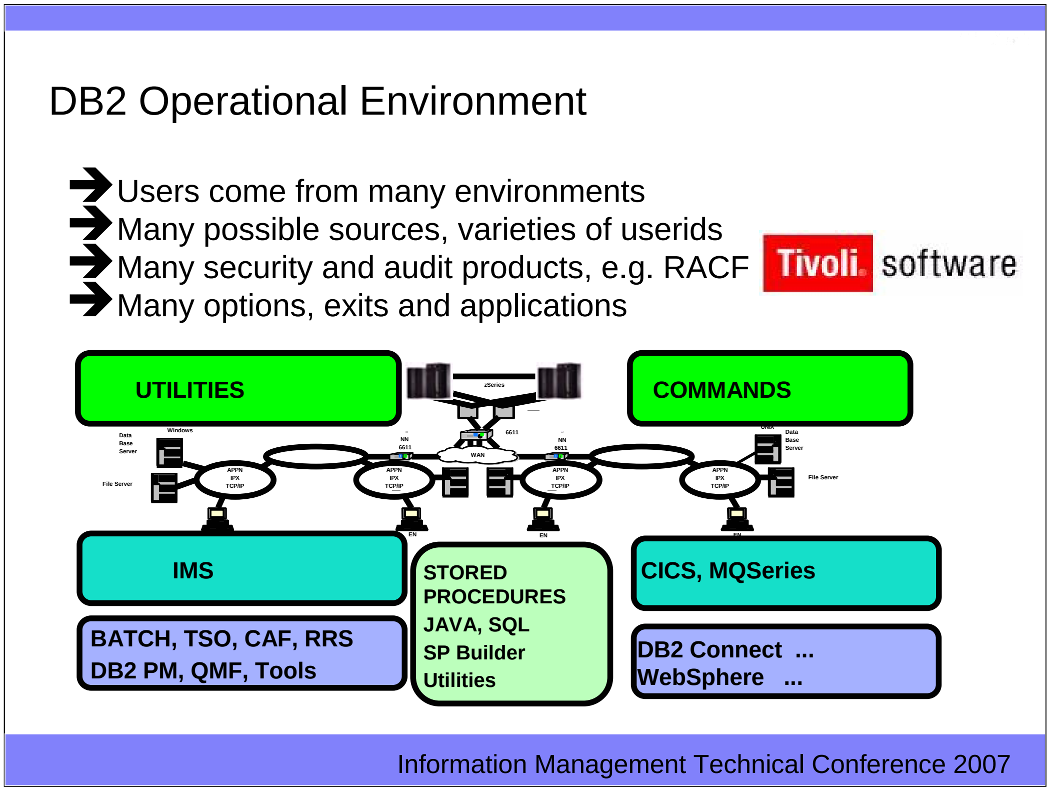
- High performance tape drive encryption
  - Cost effectively encrypt large quantities of tape data
  - Avoid Host processing encryption overhead
  - Minimize impact to existing processes and applications
- Variety of implementation methods
  - System managed
  - Library managed - TS3500 Tape Library
  - Application managed - IBM Tivoli® Storage Manager
- Supported in a wide range of environments including: z/OS™, i5/OS™, AIX®, HP, Sun, Linux and Windows

Data Encryption in TS1120
Encryption Keys
Centralized System Key Management for multiple servers
Encryption Keys
Encryption
Library Managed Encryption
TSM Application Managed Encryption

Information Management Technical Conference 2007

The IBM System Storage TS1120 Tape Drive has been enhanced to provide the customer the option of using drive based data encryption. This encryption capability is now standard on all new TS1120 Tape Drives and is a chargeable upgrade feature for existing installed TS1120 Tape Drives. The encryption capability includes drive hardware as well as microcode additions and changes. Also being introduced is a new, separate IBM Encryption Key Manager component for the Java Platform(TM) program that supports the generation and communication of encryption keys for the tape drives across the enterprise.

The TS1120 based encryption and associated Encryption Key Manager component are supported in a wide variety of operating system environments including z/OS, i5/OS, AIX, HP, Sun, Linux and Windows. In addition, three different encryption management methods are supported: Application, System, or Library Managed. This encryption capability is supported when the TS1120 Tape Drive is integrated or attaches in the IBM System Storage TS3500 Tape Library, IBM System Storage TS1120 Tape Controller Model C06, IBM TotalStorage 3592 Tape Controller Model J70, IBM TotalStorage 3494 Tape Libraries, IBM TotalStorage C20 Silo Attach frame, and standalone environments. For more information on tape encryption please see: http://www.ibm.com/servers/eserver/zseries/zos/pdf/White_Paper_ESG_System_z_final.pdf



DB2 Operational Environment

- ➔ Users come from many environments
- ➔ Many possible sources, varieties of userids
- ➔ Many security and audit products, e.g. RACF
- ➔ Many options, exits and applications

UTILITIES

COMMANDS

IMS

BATCH, TSO, CAF, RRS
DB2 PM, QMF, Tools

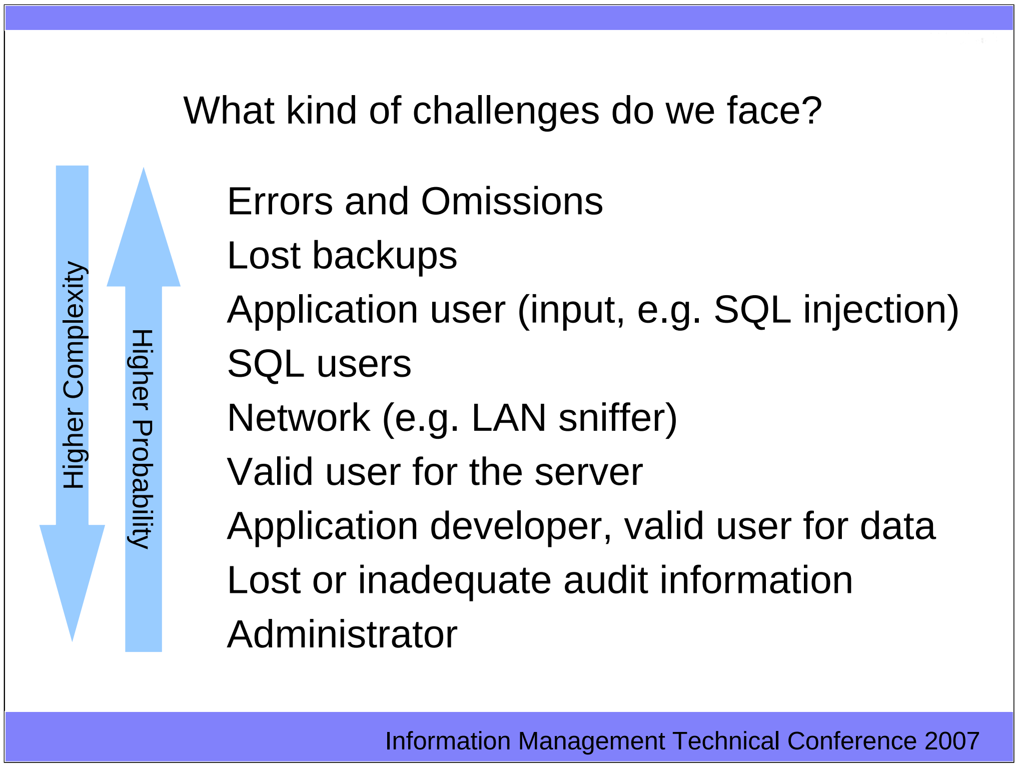
STORED PROCEDURES
JAVA, SQL
SP Builder
Utilities

CICS, MQSeries

DB2 Connect ...
WebSphere ...

There are many different environments for DB2, with different connections and security. DB2 uses the security context when possible, so batch jobs, TSO users, IMS and CICS transactions have security that uses a consistent identification and authentication. This is true for stored procedures from these environments as well. The large number of options, exits, environments and asynchronous or parallel work provide challenges for security. Some key applications manage security at the application level.

For some work, such as distributed database serving, DB2 is the initial point on this platform. For this work (DRDA distributed access, remote stored procedures), DB2 establishes the security context and manages the work.



What kind of challenges do we face?

Higher Complexity

Higher Probability

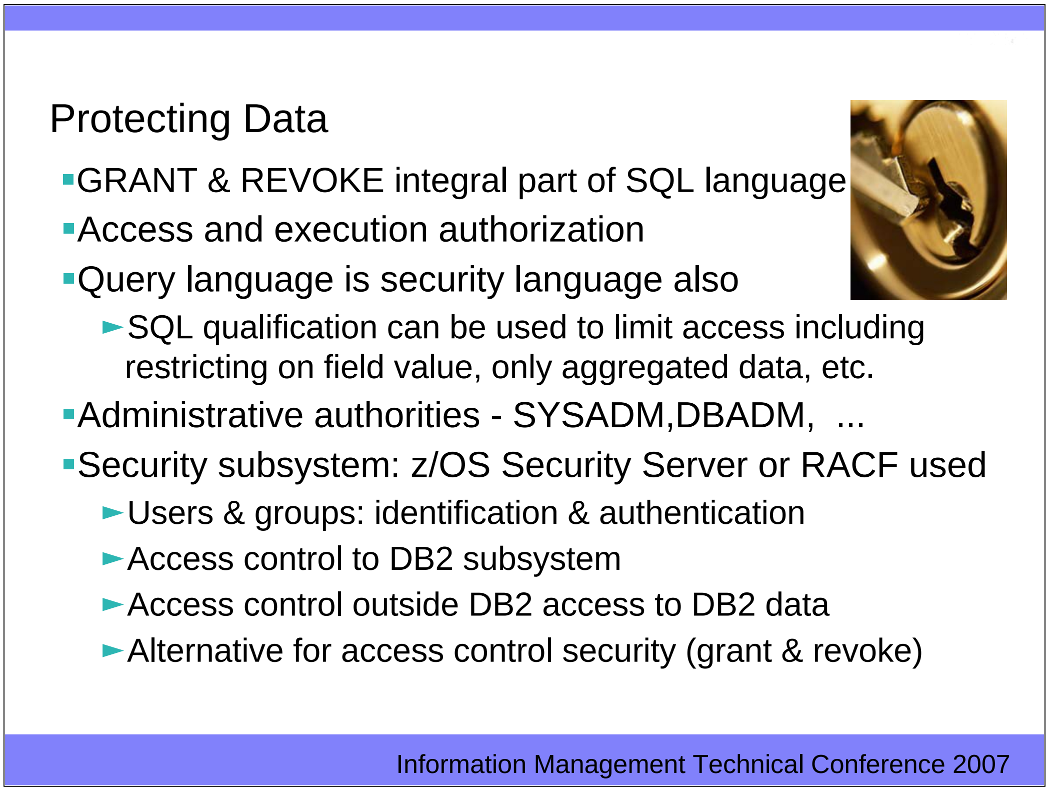
Errors and Omissions
Lost backups
Application user (input, e.g. SQL injection)
SQL users
Network (e.g. LAN sniffer)
Valid user for the server
Application developer, valid user for data
Lost or inadequate audit information
Administrator

Information Management Technical Conference 2007

See the operational environment slide for more potential of places which need to be addressed, including application code, web servers, database servers, directory and authentication devices, firewalls, network and enclave configuration and operating system platforms. It’s important to understand the other security techniques and the controls to be sure there are no gaps in the fences.

In general, we find more business losses from errors and omissions than from any other category. This area is a gateway to bigger security problems, and one that can have a very positive return on investment.

Many of the concerns are shifting from outside attacks to insiders and privileged individuals. For example, see “The Enemy Inside” CSO Magazine
http://www.csoonline.com/read/040106/caveat041206.html?source=csoupdate



Protecting Data

- GRANT & REVOKE integral part of SQL language
- Access and execution authorization
- Query language is security language also
  - SQL qualification can be used to limit access including restricting on field value, only aggregated data, etc.
- Administrative authorities - SYSADM,DBADM, ...
- Security subsystem: z/OS Security Server or RACF used
  - Users & groups: identification & authentication
  - Access control to DB2 subsystem
  - Access control outside DB2 access to DB2 data
  - Alternative for access control security (grant & revoke)

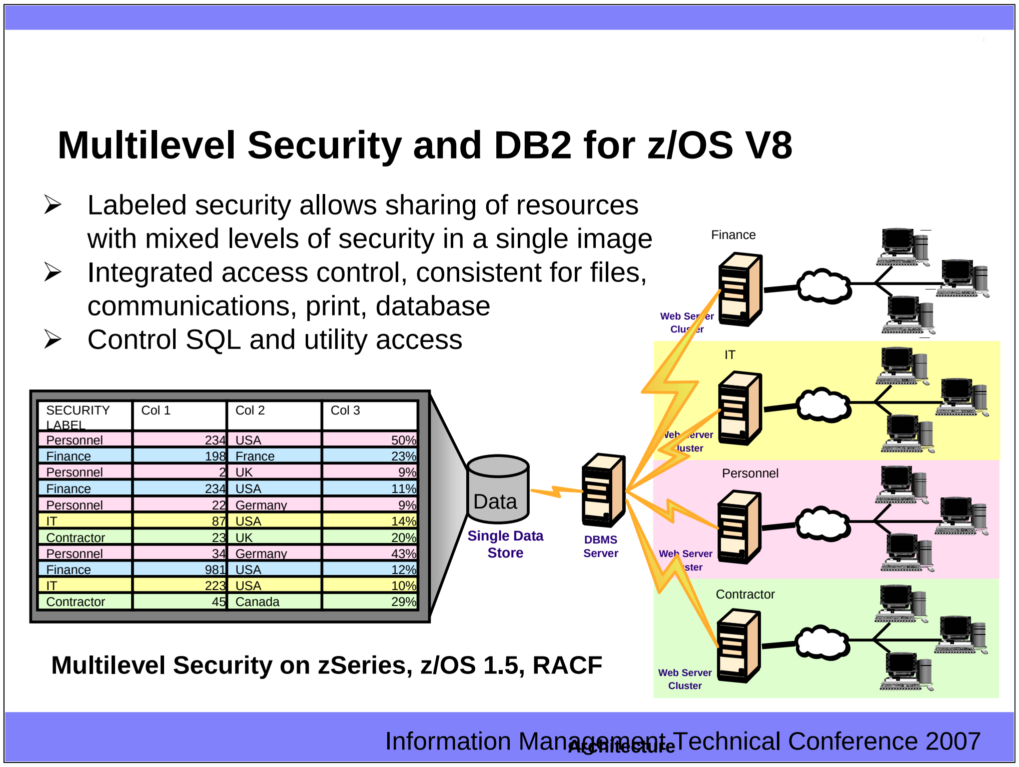
The GRANT and REVOKE SQL statements are an integral part of the SQL language and SQL standards.

Both direct data access and indirect or plan execution are included in the controls.

Views provide the ability to include a wide range of restrictions that are enforced by the DBMS.

The administrative authorities were modeled upon DBAs and system administrators, but variations in job responsibilities are common.

A security subsystem provides key parts of identification, authentication, access control and data protection, working with DB2. There is an option to use RACF or the Security Server for access control. For a detailed look at access control, see the security section of the DB2 Information Roadmap, especially the Protect Your Assets presentation (slide 42).



Multilevel Security and DB2 for z/OS V8

- Labeled security allows sharing of resources with mixed levels of security in a single image
- Integrated access control, consistent for files, communications, print, database
- Control SQL and utility access

SECURITY LABEL	Col 1	Col 2	Col 3
Personnel	234	USA	50%
Finance	198	France	23%
Personnel	2	UK	9%
Finance	234	USA	11%
Personnel	22	Germany	9%
IT	87	USA	14%
Contractor	23	UK	20%
Personnel	34	Germany	43%
Finance	981	USA	12%
IT	223	USA	10%
Contractor	45	Canada	29%

Multilevel Security on zSeries, z/OS 1.5, RACF

Information Management Technical Conference 2007

Architecture

z/OS 1.5 and RACF 1.5 or Security Server add another type of security, called multilevel security, labeled security or mandatory access control (MAC) to our capabilities. The only option in the past with a high degree of separation has been physical separation. In the database world that might mean another machine or LPAR or perhaps another subsystem, another database or another table. With multilevel security, we still have a high degree of security even with data in the same table.

Access control is consistent across many types of resources using RACF, so that multilevel controls apply for data sets, for communications, for print and for database access – both objects and now with row level granularity. The DB2 controls are for both SQL access and for utility access.

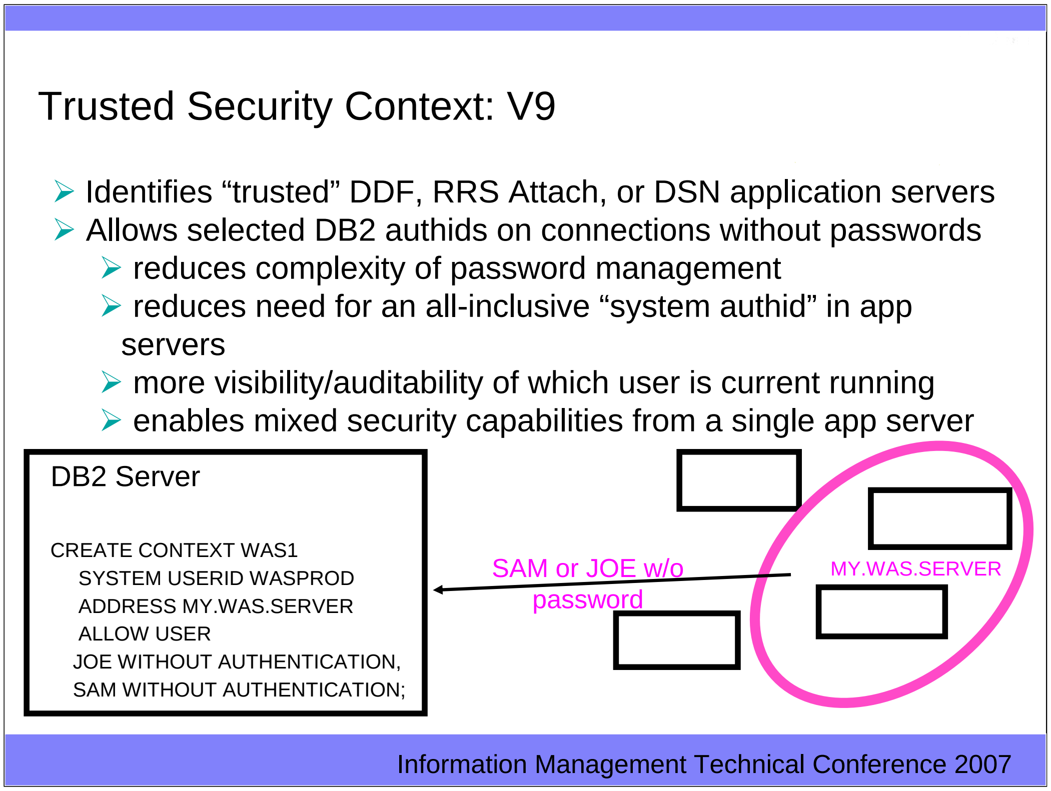
For an more on multilevel security, see **Planning for Multilevel Security and Common Criteria (GA22-7509)**

http://publibz.boulder.ibm.com/epubs/pdf/e0z2e122.pdf

Multilevel Security and DB2 Row-Level Security Revealed, SG24-6480

http://www.redbooks.ibm.com/redpieces/pdfs/sg246480.pdf

http://www.ibm.com/systems/z/security/mls.html



Trusted Security Context: V9

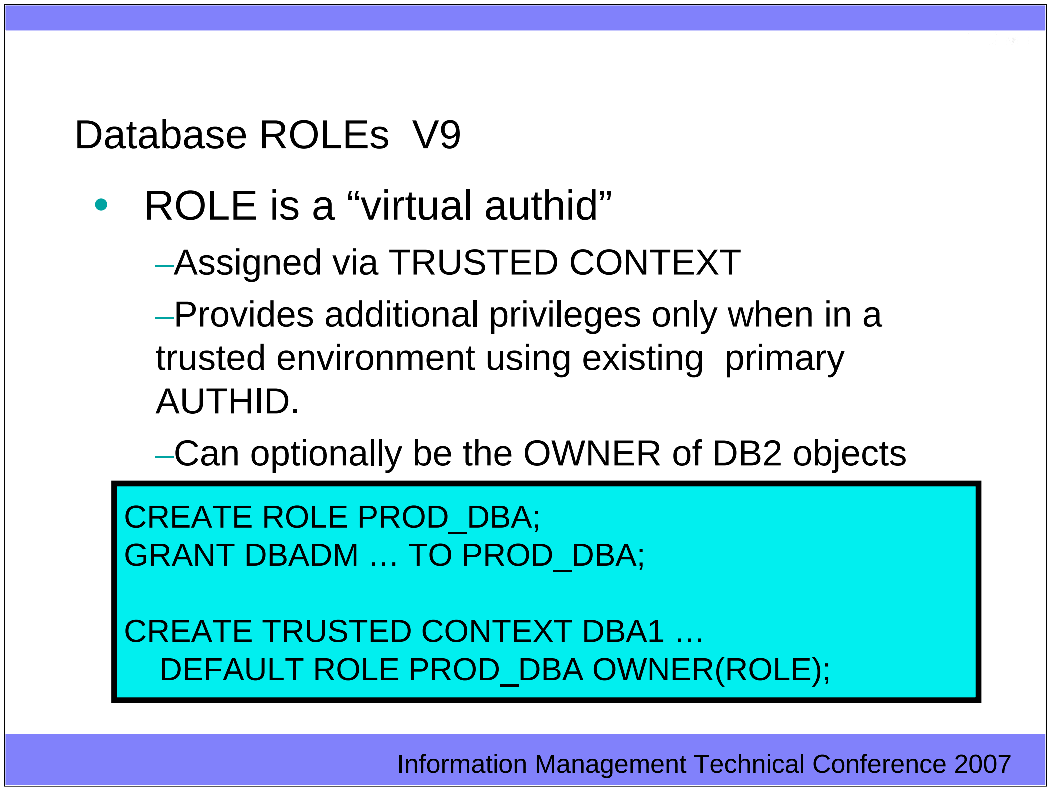
- Identifies "trusted" DDF, RRS Attach, or DSN application servers
- Allows selected DB2 authids on connections without passwords
  - reduces complexity of password management
  - reduces need for an all-inclusive "system authid" in app servers
  - more visibility/auditability of which user is current running
  - enables mixed security capabilities from a single app server

DB2 Server

```
CREATE CONTEXT WAS1
    SYSTEM USERID WASPROD
    ADDRESS MY.WAS.SERVER
    ALLOW USER
   JOE WITHOUT AUTHENTICATION,
   SAM WITHOUT AUTHENTICATION;
```

Trusted security context: Today, you have the option to set a system parameter which indicates to DB2 that all connections are to be trusted. It is unlikely that all connection types, such as DRDA, RRS, TSO, and batch, from all sources will fit into this category. It is likely that only a subset of connection requests for any type and source may be trusted or that you want to restrict trusted connections to a specific server. More granular flexibility will allow for the definition of *trusted connection objects*.

Once defined, connections from specific users via defined attachments and source servers will allow trusted connections to DB2. The users defined in this context can also be defined to obtain a *database role*.



Database ROLEs V9

- ROLE is a “virtual authid”
  - Assigned via TRUSTED CONTEXT
  - Provides additional privileges only when in a trusted environment using existing primary AUTHID.
  - Can optionally be the OWNER of DB2 objects

```
CREATE ROLE PROD_DBA;
GRANT DBADM … TO PROD_DBA;

CREATE TRUSTED CONTEXT DBA1 …
   DEFAULT ROLE PROD_DBA OWNER(ROLE);
```

Information Management Technical Conference 2007

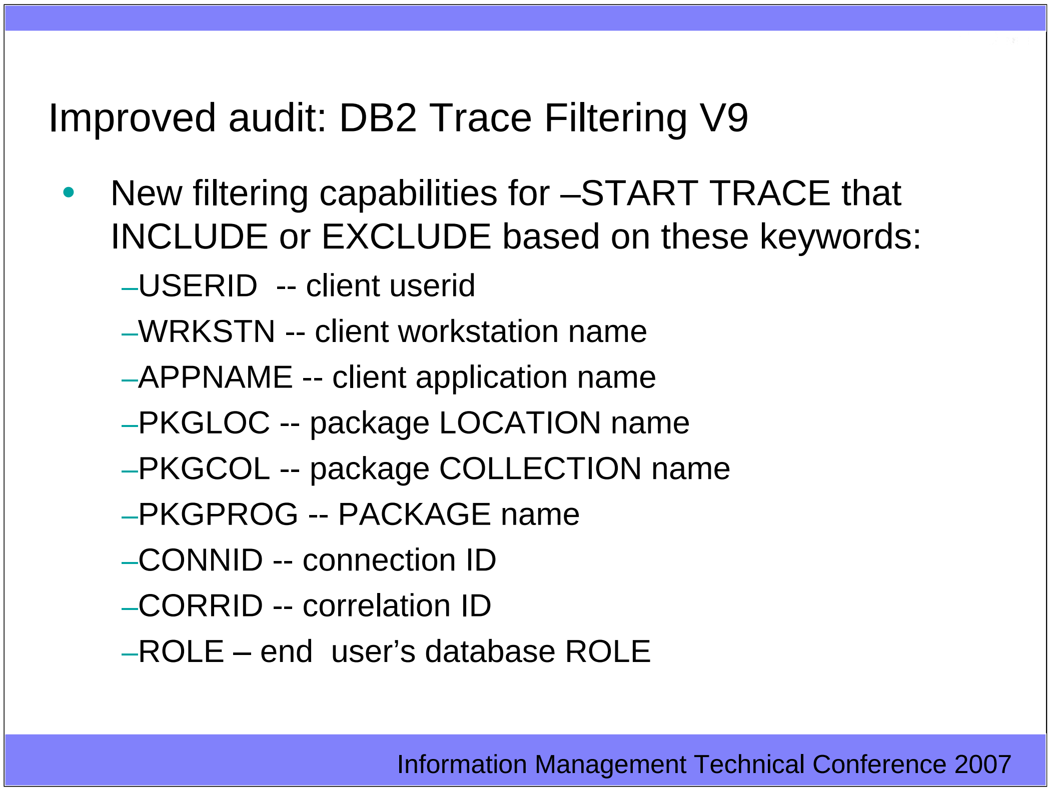
Database role: A database role is a virtual authorization ID that is assigned to the user via the context mentioned next. DB2 privileges are assigned to the defined role.

The role exists as an object independent of its creator, so creation of the role does not produce a dependency on its creator.

This capability can allow a DBA to have privileges to create objects and manage them for a time, even though ownership is to be another id.

The role can be assigned and removed from individuals via the trusted authorization context as needed. This allows a DBA to perform object maintenance during a change control window on a Saturday night, for example. But when Monday arrives, they do not have the authority to do this same work.

Auditing trails of the work completed during the maintenance window are available for verification by a security administrator or auditor.

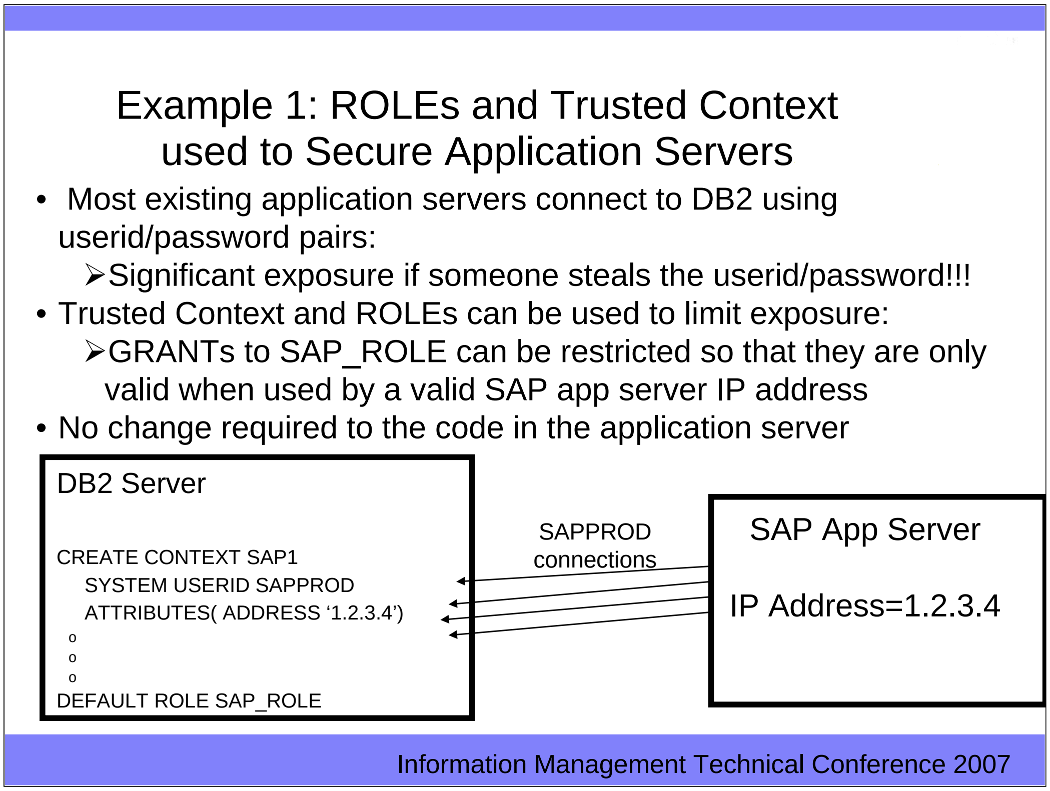


Improved audit: DB2 Trace Filtering V9

- New filtering capabilities for –START TRACE that INCLUDE or EXCLUDE based on these keywords:
  - USERID -- client userid
  - WRKSTN -- client workstation name
  - APPNAME -- client application name
  - PKGLOC -- package LOCATION name
  - PKGCOL -- package COLLECTION name
  - PKGPROG -- PACKAGE name
  - CONNID -- connection ID
  - CORRID -- correlation ID
  - ROLE – end user's database ROLE

Information Management Technical Conference 2007

Improved trace filtering makes the jobs of auditing and of performance management easier. Many more options can be used to minimize the amount of data collected, so the overhead is reduced and the extraneous data does not need to be processed.



Example 1: ROLEs and Trusted Context used to Secure Application Servers

- Most existing application servers connect to DB2 using userid/password pairs:
  - ➢Significant exposure if someone steals the userid/password!!!
- Trusted Context and ROLEs can be used to limit exposure:
  - ➢GRANTs to SAP_ROLE can be restricted so that they are only valid when used by a valid SAP app server IP address
- No change required to the code in the application server

DB2 Server

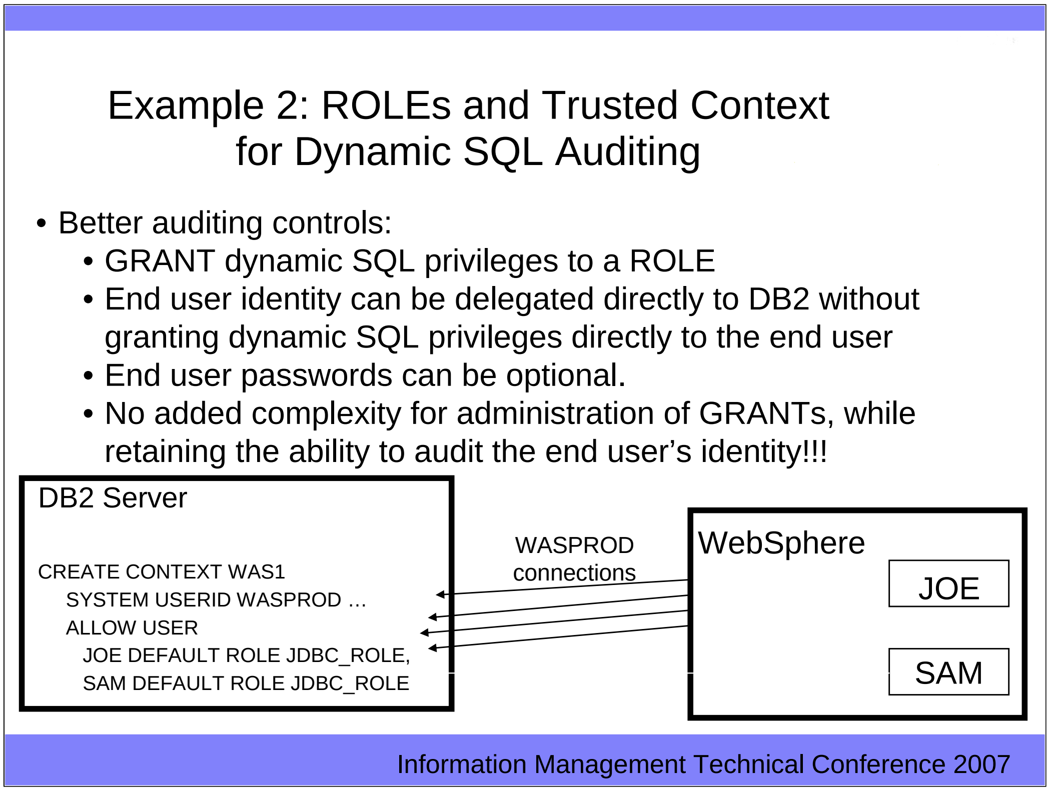
```
CREATE CONTEXT SAP1
    SYSTEM USERID SAPPROD
    ATTRIBUTES( ADDRESS ‘1.2.3.4’)
  o
  o
  o
DEFAULT ROLE SAP_ROLE
```

SAP App Server

IP Address=1.2.3.4

Information Management Technical Conference 2007

ROLEs and Trusted Context can be used to provide added security for your network-attached application servers.   These new capabilities allow the DBA to make GRANT statements conditional, so that they can only be used from a specified list of IP addresses. If someone steals the application server’s userid/password, they won’t be able to access the database unless they are also able to execute the SQL statement on one of the approved application servers.



Example 2: ROLEs and Trusted Context for Dynamic SQL Auditing

- Better auditing controls:
  - GRANT dynamic SQL privileges to a ROLE
  - End user identity can be delegated directly to DB2 without granting dynamic SQL privileges directly to the end user
  - End user passwords can be optional.
  - No added complexity for administration of GRANTs, while retaining the ability to audit the end user's identity!!!

DB2 Server

```
CREATE CONTEXT WAS1
   SYSTEM USERID WASPROD ...
   ALLOW USER
     JOE DEFAULT ROLE JDBC_ROLE,
     SAM DEFAULT ROLE JDBC_ROLE
```

WASPROD connections

WebSphere

JOE

SAM

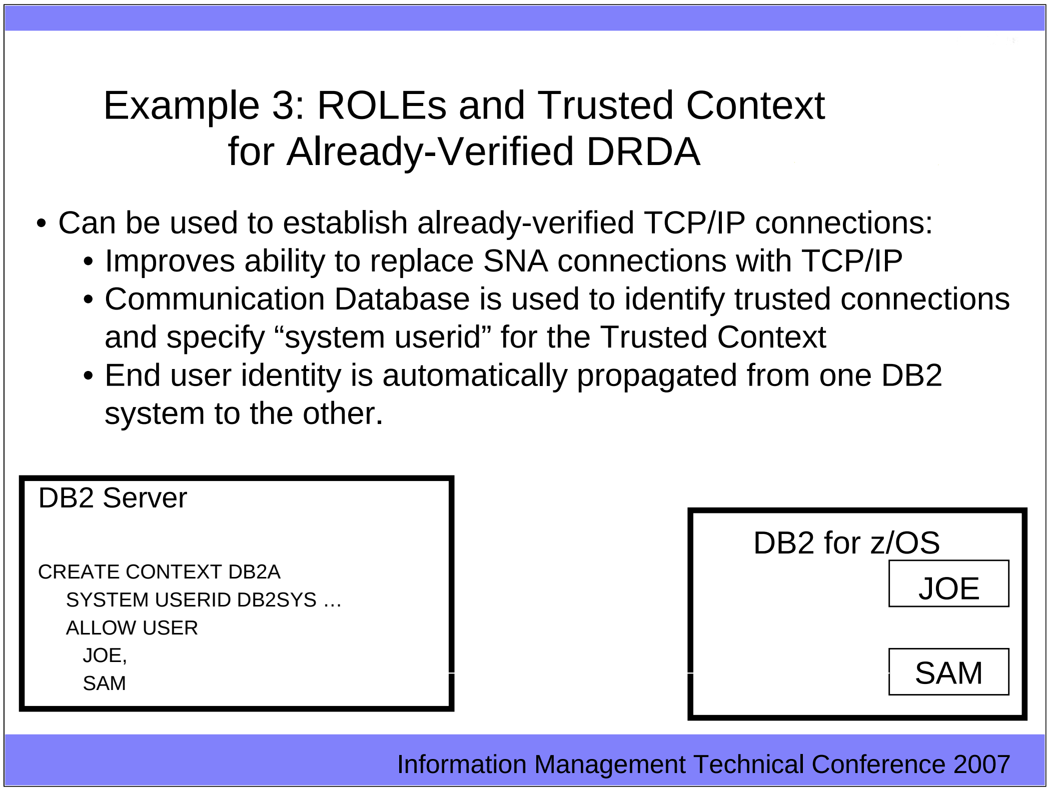
ROLEs and Trusted Context also enable customers to improve DB2 system auditing.   Today, many customers use a "system" userid to access DB2 so that they don't have to grant dynamic SQL privileges to their end users.   A second benefit to the system userid is connection pooling in the application server.

With V9, customers will be able to grant dynamic SQL table privileges to a ROLE, and specify that the end user can only use that ROLE when the end user is running on an approved application server.   This has several benefits:

•A ROLE can be used as a single database authid that can be used to simplify administration of dynamic SQL privileges.

•The end user's authid can be used to run database transactions, so that the DB2 audit is able to identify the end users individually (important capability for meeting some regulatory compliance requirements).

•The Trusted Context retains many of the performance benefits of connection pooling, while eliminating the restriction that a single authid (the system authid) must be used for all the uses of the connections in the pool.



Example 3: ROLEs and Trusted Context for Already-Verified DRDA

- Can be used to establish already-verified TCP/IP connections:
  - Improves ability to replace SNA connections with TCP/IP
  - Communication Database is used to identify trusted connections and specify “system userid” for the Trusted Context
  - End user identity is automatically propagated from one DB2 system to the other.

DB2 Server

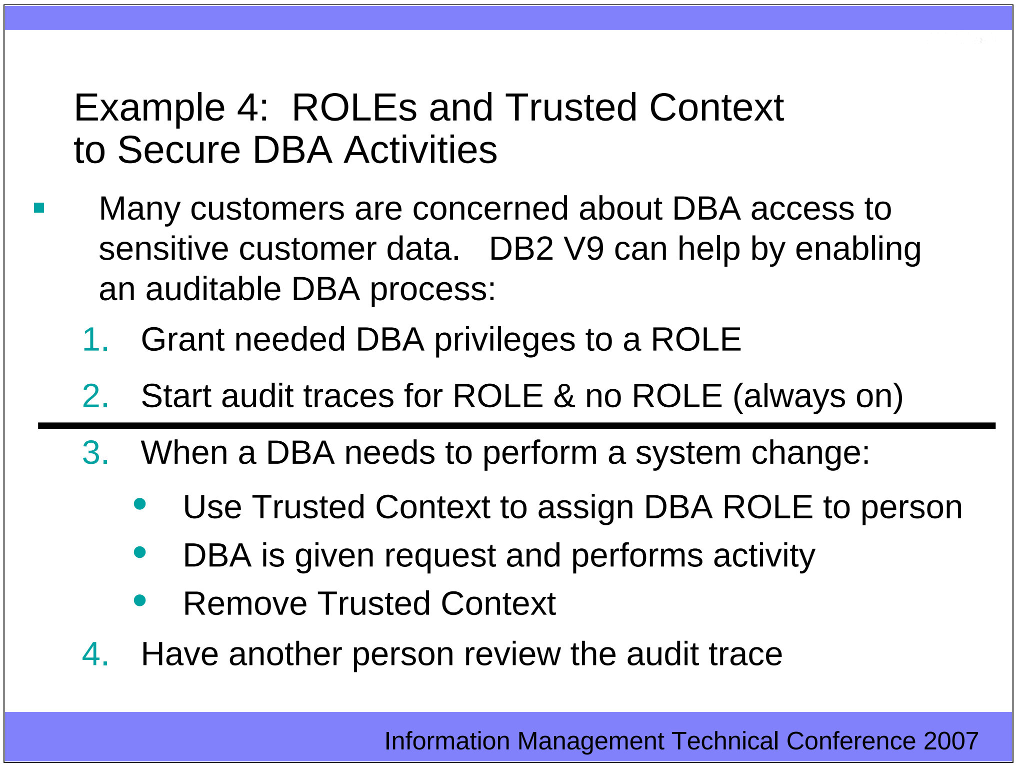
```
CREATE CONTEXT DB2A
    SYSTEM USERID DB2SYS ...
    ALLOW USER
      JOE,
      SAM
```

DB2 for z/OS

JOE

SAM

Many customers would like to migrate from SNA and PRIVATE protocol to a solution based on TCP/IP and DRDA protocol. Prior to V9, lack of already-verified support in TCP/IP prevented many customers from migrating to DRDA. With Trusted Context and changes to the Communication Database (CDB) in V9, customers will now be able to identify DB2 servers that are trusted to send already-verified connection requests.



Example 4: ROLEs and Trusted Context to Secure DBA Activities

- Many customers are concerned about DBA access to sensitive customer data. DB2 V9 can help by enabling an auditable DBA process:

1. Grant needed DBA privileges to a ROLE
2. Start audit traces for ROLE & no ROLE (always on)

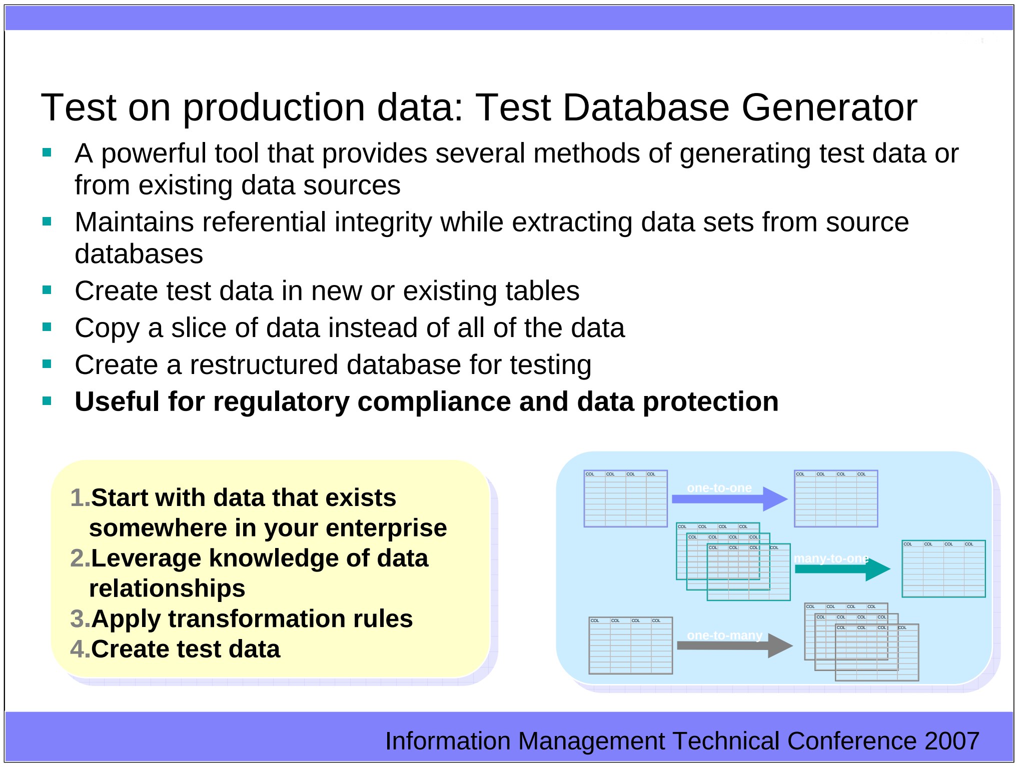
---

3. When a DBA needs to perform a system change:
   - Use Trusted Context to assign DBA ROLE to person
   - DBA is given request and performs activity
   - Remove Trusted Context
4. Have another person review the audit trace

Information Management Technical Conference 2007

The Trusted Context and ROLE support can be used to implement DBA privileges that can easily be disconnected and reconnected to individual employees. This provides function similar to shared SYSADM or DBADM userids, but avoids the audit compliance problems associated with shared userids. The ROLEs have the ability to “own” DB2 objects, so that revoking a person’s ROLE does not cause the objects to be cascade deleted.

With these capabilities, customers are able to create DBA procedures that can be audited and protected so that one individual cannot violate the established rules without being detected during the audit review.



Test on production data: Test Database Generator

- A powerful tool that provides several methods of generating test data or from existing data sources
- Maintains referential integrity while extracting data sets from source databases
- Create test data in new or existing tables
- Copy a slice of data instead of all of the data
- Create a restructured database for testing
- **Useful for regulatory compliance and data protection**

1. **Start with data that exists somewhere in your enterprise**
2. **Leverage knowledge of data relationships**
3. **Apply transformation rules**
4. **Create test data**

Information Management Technical Conference 2007

Another compliance challenge is in dealing with data for application testing. You need representative data for application testing, but you need to make sure that personal and confidential data is not easily identified. You want to take this process off the plate for auditors to look at. However, your test data still needs to be “valid”.

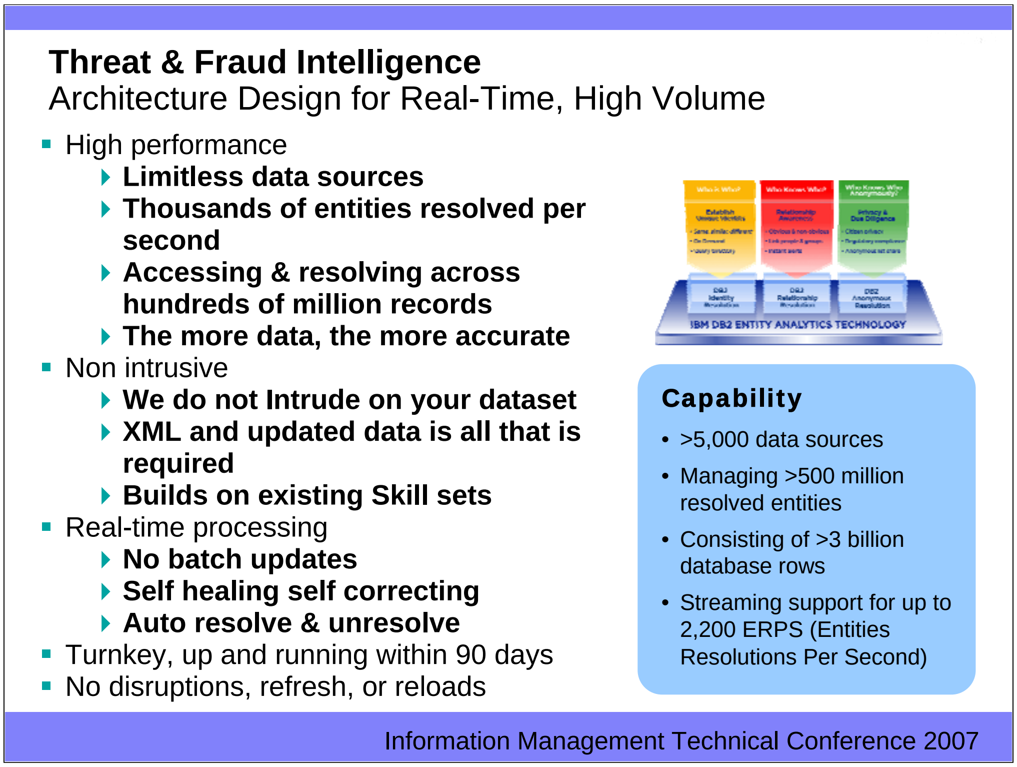
The DB2 Test Database Generator for DB2 provide an easy to use, cost effective means to help. You may have heard the famous story of the company that invested heavily in meeting regulatory compliance. They thought that they had covered everything. However the one that slipped by them was that their application developers were using copies of production data to test with. Needless to say, this was a no-no with their corporate auditors. They implemented the DB2 Test Database Generator because it could help them with:

Providing many different means for generating test data easily from scratch or from existing data sources. They used the flexibility in the tool, it has built in transformations to do things like

Random number generation, Create a target column in the test copy that generates random values for positions 1-6 of a Social Security Number, Masking of data; Create a target column that is exactly the PIN column with the 3rd and 5th positions replaced (masked) with the letter X; Data lookup: A person’s last name in a table has to be transformed into another name, but it has to be a recognizable name. You can provide a valid set of names in a lookup table and randomize within them.

The tool maintains referential integrity while extracting data from source databases. The tool uses our Grouper technology to discover non-explicitly defined relationships between objects. When testing applications, you want to make sure that you haven’t missed anything

An example: The order number in a table has to be changed to another number. This should also be applied to any dependent tables. The transformations in the DB2 Test Database Generator allowed them to generate a random number and made sure the dependent tables used the same order number. Useful for regulatory compliance and plain data protection purposes



Who is Who?
Who Knows Who?
Who Knows Who Anonymously?
Relationship Awareness
Privacy & Due Diligence
Same, similar, different
Obvious & non-obvious
Link people & groups
Instant alerts
Citizen privacy
Regulatory compliance
DB2 Identity Resolution
DB2 Relationship Resolution
DB2 Anonymous Resolution
IBM DB2 ENTITY ANALYTICS TECHNOLOGY

Threat & Fraud Intelligence

Architecture Design for Real-Time, High Volume

- High performance
  - **Limitless data sources**
  - **Thousands of entities resolved per second**
  - **Accessing & resolving across hundreds of million records**
  - **The more data, the more accurate**
- Non intrusive
  - **We do not Intrude on your dataset**
  - **XML and updated data is all that is required**
  - **Builds on existing Skill sets**
- Real-time processing
  - **No batch updates**
  - **Self healing self correcting**
  - **Auto resolve & unresolve**
- Turnkey, up and running within 90 days
- No disruptions, refresh, or reloads

Capability

- >5,000 data sources
- Managing >500 million resolved entities
- Consisting of >3 billion database rows
- Streaming support for up to 2,200 ERPS (Entities Resolutions Per Second)

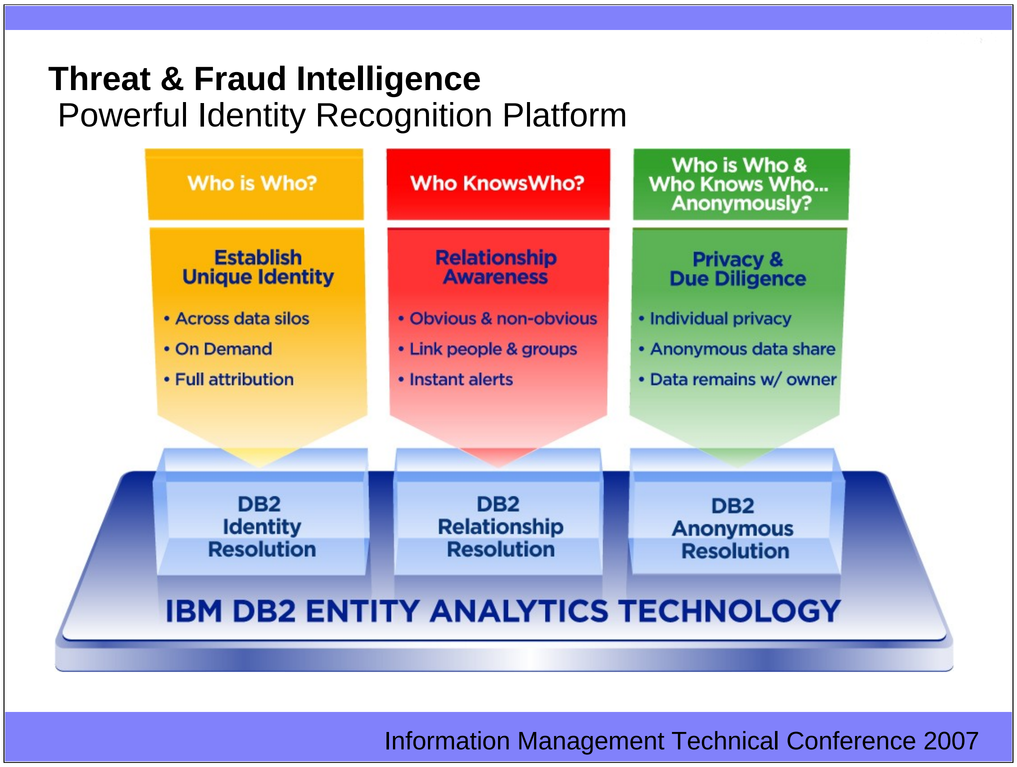
Information Management Technical Conference 2007

The problem we were asked to solve was around healthcare fraud. People were going to the hospital using their middle name instead of their first name and changing a digit in their social security number and they would not be able to be located. This technology later grows up and for the gaming industry in Las Vegas, it is used to help collapse the time between detect and preempt.

There are scams that can go down in the gaming industry that cost the organizations a quarter of a million dollars in 15 minutes. And when we did this, if you have heard about “Bringing Down the House” or the MIT team—in that book it says they wondered how it became where they could recruit a new face, a new person that no one has ever seen, and within 15 minutes of them showing up in the casino, they would be detected and removed. And this technology played a role in that. In the late ‘90s, a consumer conglomerate used the technology to amass data of about a hundred million consumers across 4,200 disparate systems to understand when people were the same.

It is for marketing purposes. It ensures that nobody sends me hair care products. Then this technology starts being used by the government for insider threats. The costs of insiders to an organization can be enormous. And today the technology is used not only for national security purposes. I could tell you but I would have to kill you. But also in financial services, retail, and things like that.

There are three products in our suite. We are, by the way, the SRD Company. We are still located in Las Vegas and we are now the Entity Analytics Solution Group or sometimes EAS. Our base core technology is about identity resolution. Figuring out when two people are the same despite all of the natural variability in data. You know, Jeff with the J, Geoff with the G, 128 spellings of Mohammed. What is unique about this technology is that it is not about how two lists compare. It is not about Dataset A, Dataset B and seeing what it means when you put them together because sometimes it is a third or fourth piece of data that is the glue that allows you to put the data together.



Threat & Fraud Intelligence

Powerful Identity Recognition Platform

Who is Who?

Establish Unique Identity

- Across data silos
- On Demand
- Full attribution

Who KnowsWho?

Relationship Awareness

- Obvious & non-obvious
- Link people & groups
- Instant alerts

Who is Who & Who Knows Who... Anonymously?

Privacy & Due Diligence

- Individual privacy
- Anonymous data share
- Data remains w/ owner

DB2 Identity Resolution

DB2 Relationship Resolution

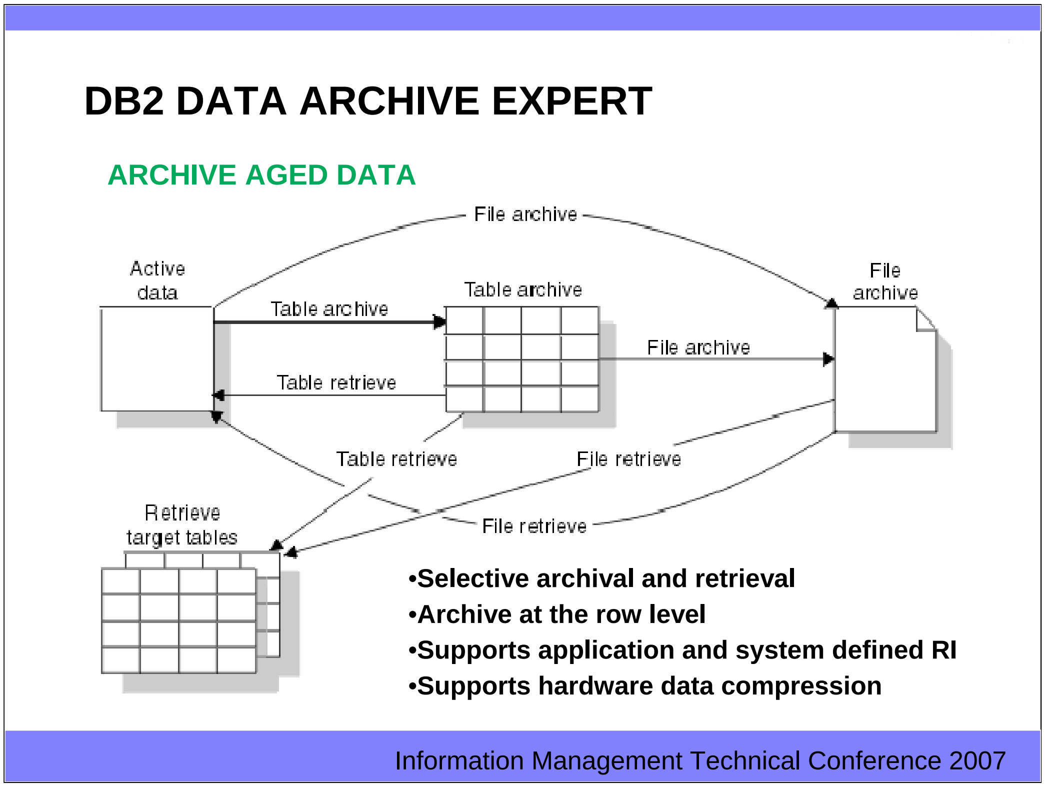
DB2 Anonymous Resolution

IBM DB2 ENTITY ANALYTICS TECHNOLOGY

Information Management Technical Conference 2007

IBM has solutions that facilitate the identification of employees and customers intent on doing harm. Taking advantage of entity analytics, healthy hospitality companies detect and identify internal fraud, collusion and embezzlement. They can detect and identify employee/vendor collusion and excluded vendors. These solutions can also support the Sarbanes-Oxley and U.S. Patriot Acts; stop money laundering; and detect and identify casino cheats, criminals and gaming control arrestees. What’s more, they can aid in risk management involving criminals, terrorists, workplace violence and organized crime.

IBM Entity Analytic Solutions (EAS) offers the only technology designed to provide a real-time, total view of information to resolve individual identity and relationships. EAS clients leverage these solutions to recognize internal and external threats, and to share this information anonymously.



DB2 DATA ARCHIVE EXPERT

ARCHIVE AGED DATA

- •Selective archival and retrieval
- •Archive at the row level
- •Supports application and system defined RI
- •Supports hardware data compression

Information Management Technical Conference 2007

Many if not most of the regulations these days require a retention period for data. Often this period is 7 or more years. In many cases it does not make sense to keep this data with your active production data for cost and security purposes. Also, these same regulations require you to be able to demonstrate a systematic (and auditable) approach to archiving. This is not always easy to do with individual applications groups responsible for archiving data. This is where a tool like the DB2 Data Archive Expert for DB2 on z series and DB2 on LUW can play an important, centralized role.

The tool allows you to archive and retrieve sets of information across multiple tables. It allows you to set profiles to selectively identify data to archive and retrieve. This gives the archiving process an application, or row based, basis for archiving while meeting the requirements of a systematic approach

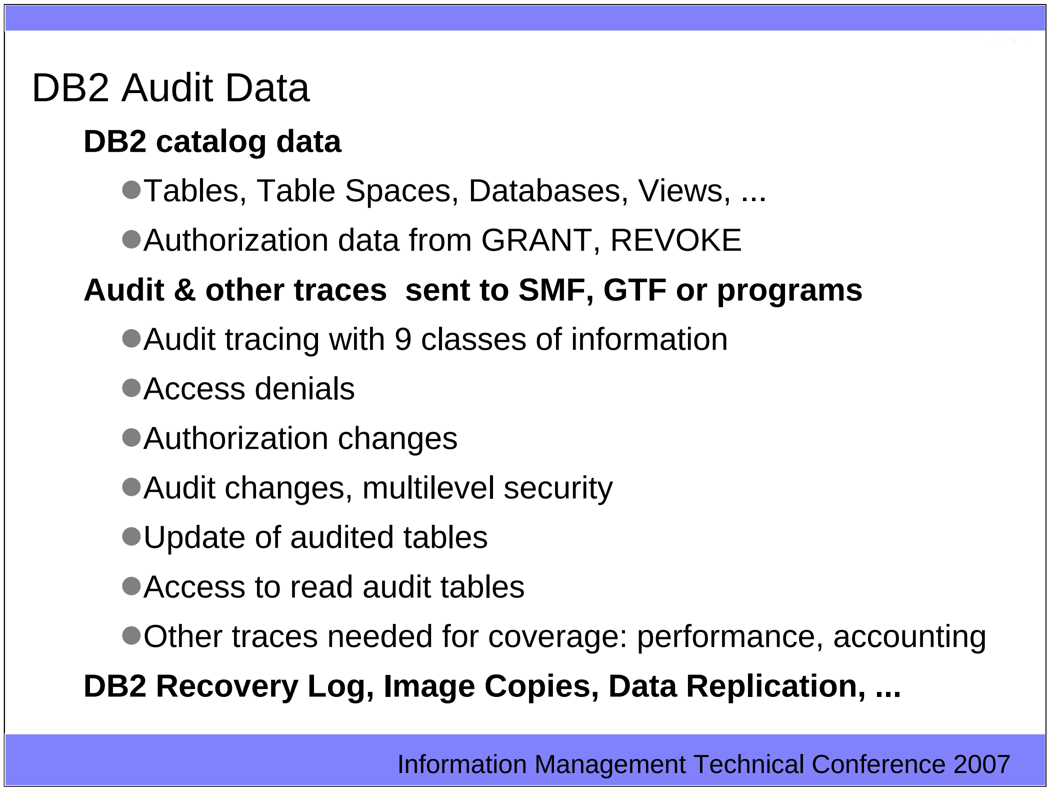
The tool provide a choice of archiving strategies --

To table, to file, or to both (multi-tier).

In the case of archiving to tables, access to archived data with SQL can be accomplished with minimal or no application changes. It uses the Grouper component to ensure that you are archiving related objects together, supporting application and system defined RI. Again, auditors don't look favorably on archiving only portions of critically related data

You have the option of deleting the archived data from the active repositories or deferring the deletion until later. Supports hardware data compression for compression of archived copies

ftp://ftp.software.ibm.com/software/db2storedprocedure/db2zos390/techdocs/F05m.pdf



DB2 Audit Data

DB2 catalog data

- Tables, Table Spaces, Databases, Views, ...
- Authorization data from GRANT, REVOKE

Audit & other traces sent to SMF, GTF or programs

- Audit tracing with 9 classes of information
- Access denials
- Authorization changes
- Audit changes, multilevel security
- Update of audited tables
- Access to read audit tables
- Other traces needed for coverage: performance, accounting

DB2 Recovery Log, Image Copies, Data Replication, ...

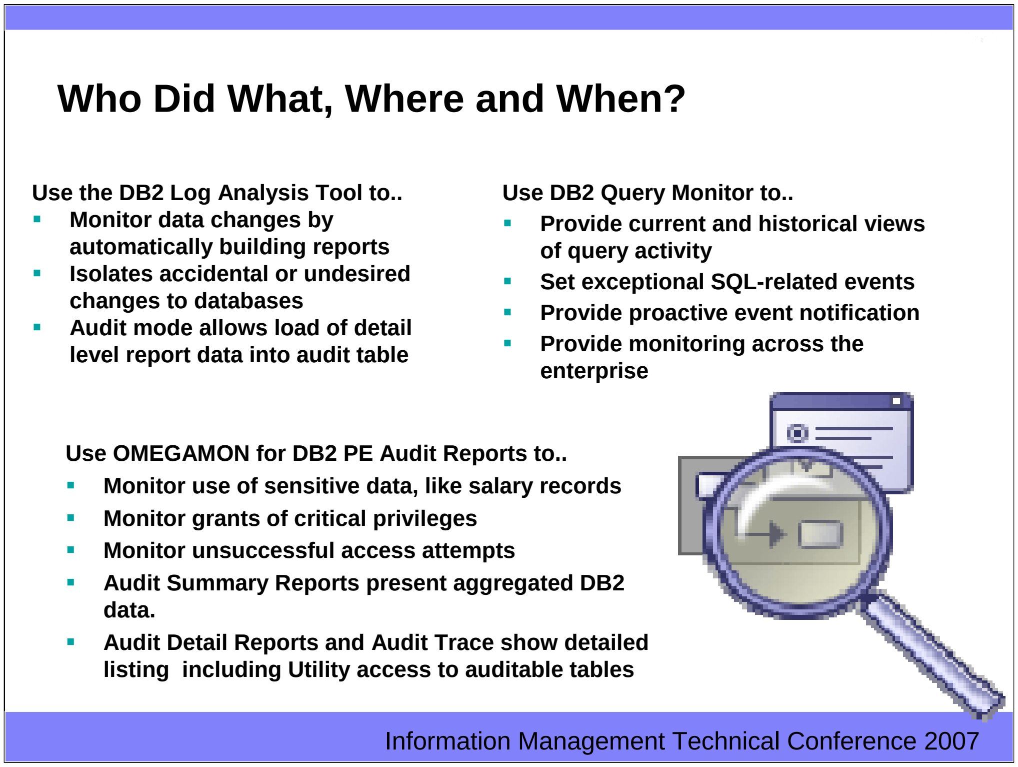
Information Management Technical Conference 2007

There are many kinds of audit information available in DB2. The DB2 catalog stores the definitions of all the objects and the authorization. Users who are allowed to access these tables can use the power of SQL to audit and manage security. RACF has an unload facility that allows its security definitions to be loaded into DB2, so that broader auditing can be performed.

One of the primary audit sources is an audit trace that can provide very selective information. Other trace information can also be used in auditing.

The DB2 recovery log and utilities are also helpful in finding out how and when some data was modified.

Please read the Audit section of the Security and Auditing chapter of the DB2 Administration Guide.



Who Did What, Where and When?

Use the DB2 Log Analysis Tool to..

- Monitor data changes by automatically building reports
- Isolates accidental or undesired changes to databases
- Audit mode allows load of detail level report data into audit table

Use DB2 Query Monitor to..

- Provide current and historical views of query activity
- Set exceptional SQL-related events
- Provide proactive event notification
- Provide monitoring across the enterprise

Use OMEGAMON for DB2 PE Audit Reports to..

- Monitor use of sensitive data, like salary records
- Monitor grants of critical privileges
- Monitor unsuccessful access attempts
- Audit Summary Reports present aggregated DB2 data.
- Audit Detail Reports and Audit Trace show detailed listing including Utility access to auditable tables

Information Management Technical Conference 2007

IBM Tools for DB2 can help you to manage some of the costly parts of meeting regulatory compliance in encryption, protection of sensitive data, retaining data for audits. Next lets look at ability to audit the systems - discovering who did what, where and when in real time and historically.

Today in our tools suite we have products that give you this ability. Tools like the DB2 Log Analysis Tool. This tool audit the DB2 logs and build reports to detect undesired changes to databases.

The DB2 Query Monitor provides details on read activity and can be used to set exceptions based upon undesirable SQL access to data objects.

You can use the Tivoli OMEGAMON XE for DB2 PE audit reports to monitor usage of sensitive data, like employee salary records. Use it to monitor grants of critical privileges and unsuccessful access attempts to sensitive data including, utility access to auditable tables.

DB2 Audit Management Expert for z/OS V1.1

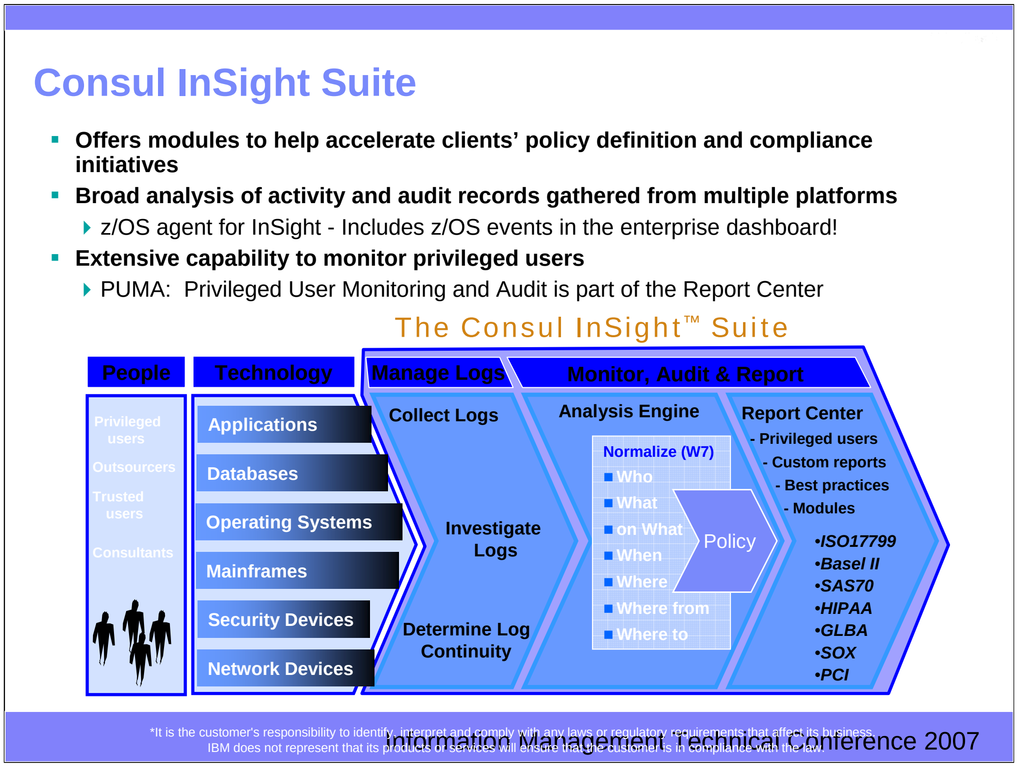
- Focus on aiding compliance with plethora of regulations
  - ►Sarbanes – Oxley
  - ►Basel II
  - ►HIPAA
  - ►Japanese "Protecting Personal Freedom" Act
  - ►Many others…
- Useful for both **DBAs** and **Corporate Auditors**
  - ►Monitoring and reporting for both Access and Change
  - ►"After the fact" (log access) reporting
  - ►Various filtering available - object name, user name, program, etc.
  - ►Maintain history or access directly
  - ►Uses DB2 trace records

Information Management Technical Conference 2007

Auditing is a complicated process. Auditors often are not experts on DB2 or on determining which objects to audit, starting appropriate traces, collecting and filtering and producing reports. Auditors rely heavily upon the DBA staff. Still, executives are explicitly responsible for providing accurate, reliable, and timely information to the public and auditors are charged with the responsibility of ensuring that the audit is effective.

This is why we provided a comprehensive auditing solution to make auditing, and the jobs of DBAs who support auditors, much easier. Collecting the data is complicated. This tool makes it easier. Data collection would be better in a central repository for collected audit data. Auditors must be able to access SELECT, INSERT, UPDATE, and DELETE activity by user or by object. Auditors need to have easy to see graphical and batch reports for auditable activity. Auditors and users of this tool do not have to be DB2 experts and the tool makes life easier for the DBAs that support audit. This tool, the DB2 Audit Management Expert for z/OS V1.1 is now available.

This webcast describes the product:
http://www.ibm.com/software/os/zseries/telecon/14sep/



Consul InSight Suite

- Offers modules to help accelerate clients' policy definition and compliance initiatives
- Broad analysis of activity and audit records gathered from multiple platforms
  - z/OS agent for InSight - Includes z/OS events in the enterprise dashboard!
- Extensive capability to monitor privileged users
  - PUMA: Privileged User Monitoring and Audit is part of the Report Center

The Consul InSight™ Suite

People

Privileged users

Outsourcers

Trusted users

Consultants

Technology

Applications

Databases

Operating Systems

Mainframes

Security Devices

Network Devices

Manage Logs

Collect Logs

Investigate Logs

Determine Log Continuity

Monitor, Audit & Report

Analysis Engine

Normalize (W7)

- Who
- What
- on What
- When
- Where
- Where from
- Where to

Policy

Report Center

- Privileged users
- Custom reports
- Best practices
- Modules

•*ISO17799*
•*Basel II*
•*SAS70*
•*HIPAA*
•*GLBA*
•*SOX*
•*PCI*

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Information Management Technical Conference 2007

Consul's InSight Suite addresses compliance monitoring, auditing and reporting. InSight Suite is a distributed environment solution that takes info across the enterprise, and integrates with the zAudit functionality for the mainframe. Mainframe information is fed into the InSight Suite GUI for ease of use; InSight takes the primary audit trail of z/OS, SMF.

Single interface can do reporting, semi-annual audits, daily monitoring, across entire system config. Note that InSight pulls in System z data as well for true end-to-end comprehensive reporting

- Patent-pending W7 (who, what, on what, when, where, where from, where to) methodology for analysis that you can see on the chart
- Out-of-the-box compliance support modules, that you can also see on the chart to the far right, are key to helping accelerate clients' policy & compliance initiatives

Consul enhances security management

    1. Key point - mainframe

1. Consul adds innovative compliance management

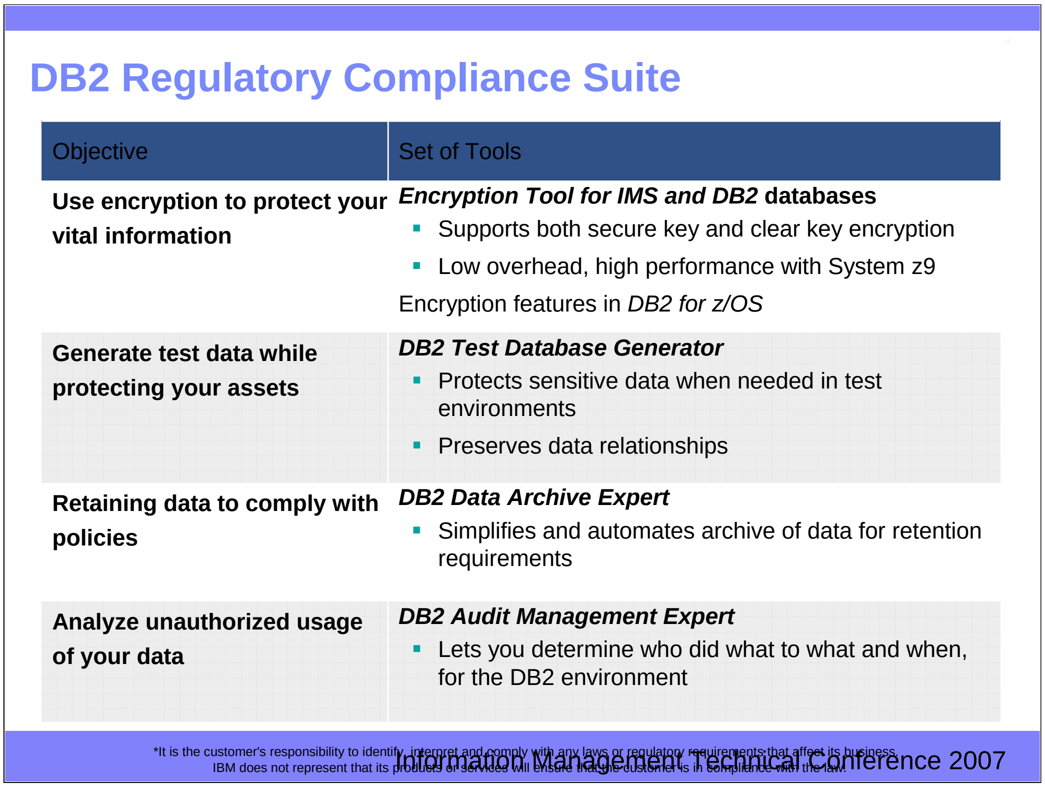
    1. Key point – compliance modules

Include z/OS events into InSight reports

    z/OS, RACF, CA-ACF2, CA-Top Secret, DB2

Translate MVS jargon into InSight's compliance language

Auditors no longer need z/OS expertise to monitor activities



DB2 Regulatory Compliance Suite

Objective	Set of Tools
Use encryption to protect your vital information	***Encryption Tool for IMS and DB2* databases** - Supports both secure key and clear key encryption - Low overhead, high performance with System z9 Encryption features in *DB2 for z/OS*
Generate test data while protecting your assets	***DB2 Test Database Generator*** - Protects sensitive data when needed in test environments - Preserves data relationships
Retaining data to comply with policies	***DB2 Data Archive Expert*** - Simplifies and automates archive of data for retention requirements
Analyze unauthorized usage of your data	***DB2 Audit Management Expert*** - Lets you determine who did what to what and when, for the DB2 environment

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Information Management Technical Conference 2007

Effectively responding to data compliance and privacy regulations is a top concern for most IT professionals today - adding new levels of complexity around data management. Concerns they share include: -How do I determine who made changes to my companies data and when?

-I am now required to maintain more data for longer periods of time.

- How can I easily move that data to less expensive disk or Tape while still making it available to end users and auditors?

-Are my developers using production data for testing purposes? If yes, how do I protect sensitive data while still using it to provide valid test scenarios?

-How do I protect data when it is moved from location to location?

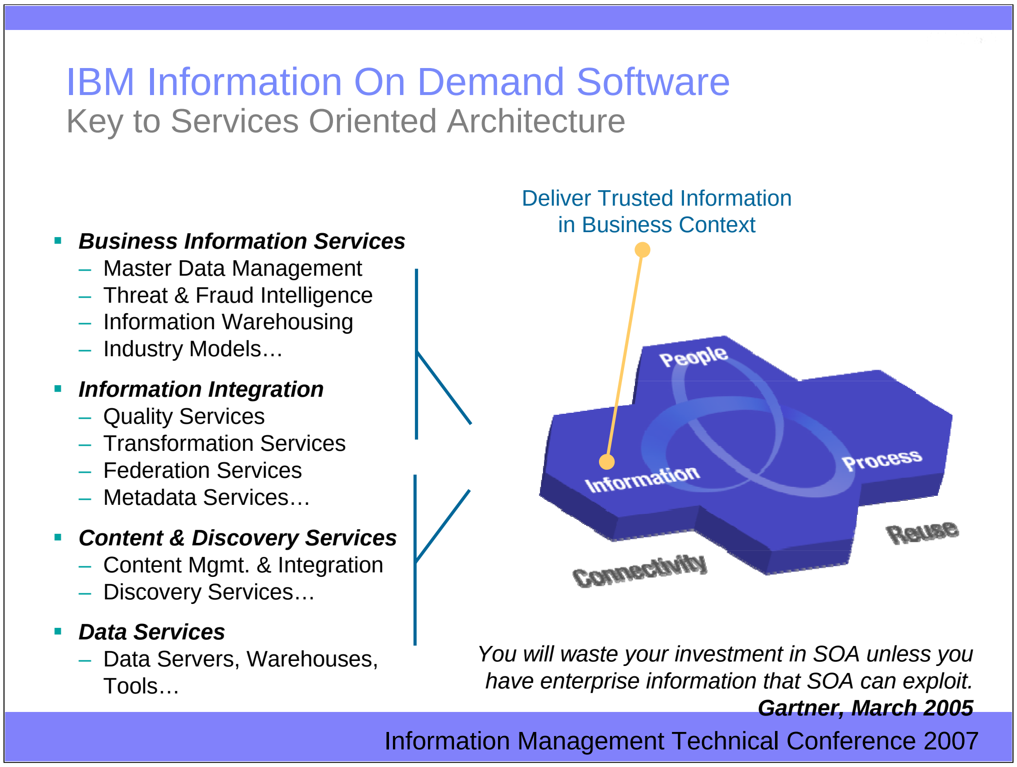
IBM offers a suite of compliance product offerings to address these high priority concerns. We expect this set of products will be very useful to many corporations for whom regulatory compliance is an increasingly time consuming and expensive task.

The IBM Data Encryption for IMS and DB2 Databases provides you with a data encryption tool for both IMS and DB2 for z/OS databases in a single product. This product is designed to enable you to protect sensitive and private data for IMS at the segment level and for DB2 at the row level. IBM Data Encryption for IMS and DB2 Databases is implemented via standard IMS and DB2 exits which invoke System z cryptography hardware to encrypt data for storage and decrypt data for application use. Click here to examine how IBM Data Encryption for IMS and DB2 Databases can help.

http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html

DB2 Test Database Generator

To help you deal with the routine task of creating test data IBM offers DB2 Test Database Generator for the z/OS as well as the Linux, Unix and Microsoft Windows environments. This tool helps both developers and database administrators quickly create test data from scratch or



IBM Information On Demand Software

Key to Services Oriented Architecture

- ***Business Information Services***
  - Master Data Management
  - Threat & Fraud Intelligence
  - Information Warehousing
  - Industry Models…
- ***Information Integration***
  - Quality Services
  - Transformation Services
  - Federation Services
  - Metadata Services…
- ***Content & Discovery Services***
  - Content Mgmt. & Integration
  - Discovery Services…
- ***Data Services***
  - Data Servers, Warehouses, Tools…

Deliver Trusted Information in Business Context

You will waste your investment in SOA unless you have enterprise information that SOA can exploit.
Gartner, March 2005

Information Management Technical Conference 2007

We are seeing a convergence of data for managing the company, with business intelligence, business performance management and compliance often looking for similar information. The Information on Demand structure can be used to provide consistent information to a wide group of people in a convenient form. The IBM Information Management product structure includes the broader range of capabilities.

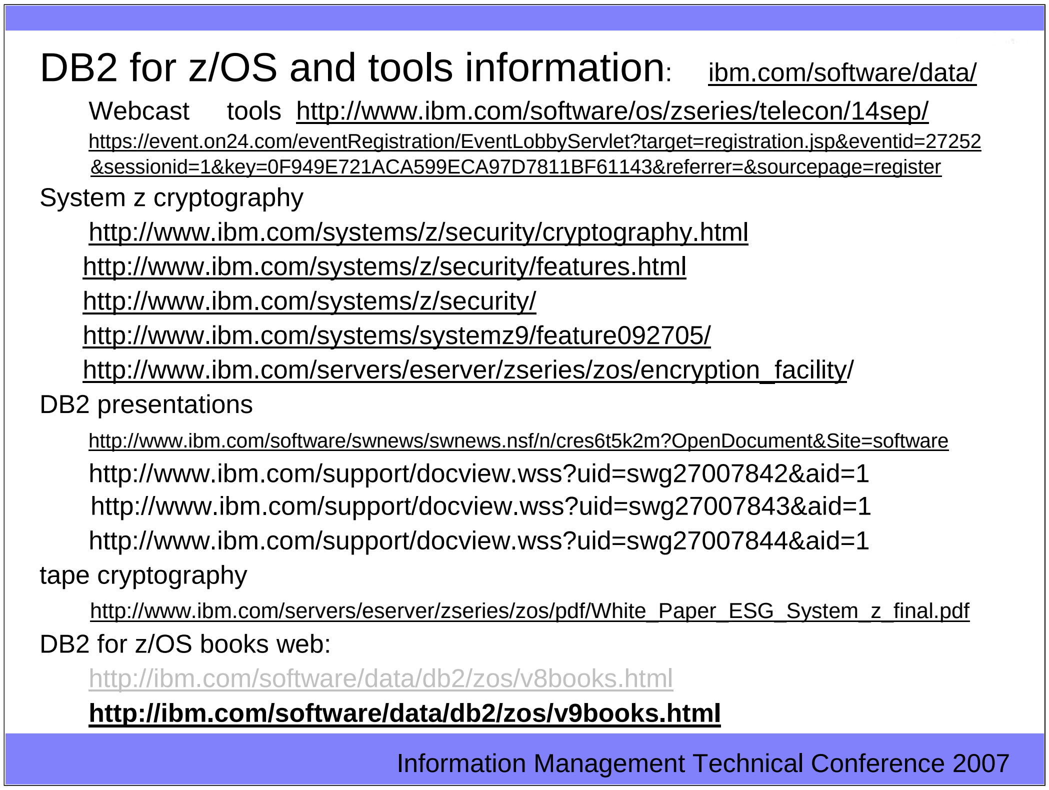
Another part of our investment is to take these services and make them available in the context of a services oriented architecture.

business flexibility because processes are composed of granular, reusable services, shared across the entire business and based on open standards like XML and web services.

Information On Demand is key to SOA.

> Processes composed of granular, reusable services need unified, trusted information that is delivered in the context of the process being composed…

Together, SOA and Information On Demand, as well as collaborative tools for people, deliver the business flexibility demanded in today’s world.



DB2 for z/OS and tools information: ibm.com/software/data/

Webcast tools http://www.ibm.com/software/os/zseries/telecon/14sep/
https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27252&sessionid=1&key=0F949E721ACA599ECA97D7811BF61143&referrer=&sourcepage=register

System z cryptography

http://www.ibm.com/systems/z/security/cryptography.html
http://www.ibm.com/systems/z/security/features.html
http://www.ibm.com/systems/z/security/
http://www.ibm.com/systems/systemz9/feature092705/
http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/

DB2 presentations

http://www.ibm.com/software/swnews/swnews.nsf/n/cres6t5k2m?OpenDocument&Site=software
http://www.ibm.com/support/docview.wss?uid=swg27007842&aid=1
http://www.ibm.com/support/docview.wss?uid=swg27007843&aid=1
http://www.ibm.com/support/docview.wss?uid=swg27007844&aid=1

tape cryptography

http://www.ibm.com/servers/eserver/zseries/zos/pdf/White_Paper_ESG_System_z_final.pdf

DB2 for z/OS books web:

http://ibm.com/software/data/db2/zos/v8books.html
http://ibm.com/software/data/db2/zos/v9books.html

Information Management Technical Conference 2007

Here are some additional pointers for information about DB2, security and compliance. Planning for Multilevel Security is on the web under z/OS library, System level books, or

ibm.com/servers/eserver/zseries/zos/bkserv/r5pdf/zsys.html

DB2 V8 and DB2 9books including the RACF Access Control Module Guide are located at

http://www.ibm.com/software/data/db2/zos/v8books.html

http://www.ibm.com/software/data/db2/zos/v9books.html

ICSF and key management:

ftp://ftp.software.ibm.com/software/mktsupport/techdocs/keymgmt.pdf

http://www.ibm.com/support/techdocs/atsmastr.nsf/fe582a1e48331b5585256de50062ae1c/eb1b01f317fa015786256dd400020e85/$FILE/zoscrypto-techdocs.pdf

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1880

http://www.ibm.com/support/techdocs/atsmastr.nsf/032f6e163324983085256b79007f5aec/09ae5cfe8c313657862570850058afa4/$FILE/Clear%20Key%20Secure%20Key%20Primer.pdf

IBM

Securing DB2 and Implementing MLS on z/OS

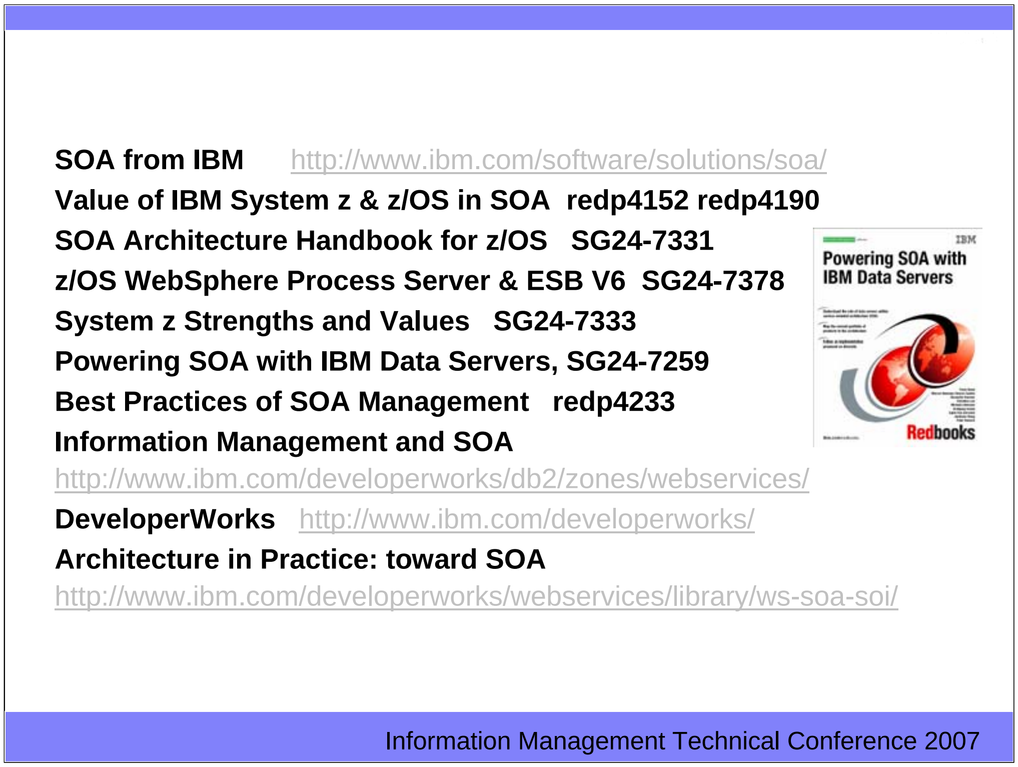
DB2 V9 trusted context and roles

Multilevel security: What, why, and how

Vanguard Administrator: Simplifying MLS implementations

Information Management Technical Conference 2007

This is the recent redbook update, SG24-6480-01, describing DB2 V8and 9 security changes.


IBM
Powering SOA with IBM Data Servers
Redbooks

SOA from IBM http://www.ibm.com/software/solutions/soa/

Value of IBM System z & z/OS in SOA redp4152 redp4190

SOA Architecture Handbook for z/OS SG24-7331

z/OS WebSphere Process Server & ESB V6 SG24-7378

System z Strengths and Values SG24-7333

Powering SOA with IBM Data Servers, SG24-7259

Best Practices of SOA Management redp4233

Information Management and SOA
http://www.ibm.com/developerworks/db2/zones/webservices/

DeveloperWorks http://www.ibm.com/developerworks/

Architecture in Practice: toward SOA
http://www.ibm.com/developerworks/webservices/library/ws-soa-soi/

Information Management Technical Conference 2007

SOA from IBM
http://www.ibm.com/jct09002c/isv/soa/resources.html
http://www.ibm.com/software/solutions/soa/

The Value of the IBM System z and z/OS in Service-Oriented Architecture
http://www.redbooks.ibm.com/abstracts/redp4152.html?Open

The Value of the IBM System z and z/OS in the Design of a Service-Oriented Architecture
http://www.redbooks.ibm.com/abstracts/redp4190.html?Open

SOA Architecture Handbook for z/OS
http://www.redbooks.ibm.com/redpieces/abstracts/sg247331.html?Open

z/OS Getting Started: WebSphere Process Server and WebSphere Enterprise Service Bus V6
http://www.redbooks.ibm.com/abstracts/sg247378.html?Open

System z Strengths and Values
http://www.redbooks.ibm.com/abstracts/sg247333.html?Open

Powering SOA with IBM Data Servers, SG24-7259
http://www.redbooks.ibm.com/abstracts/sg247259.html?Open

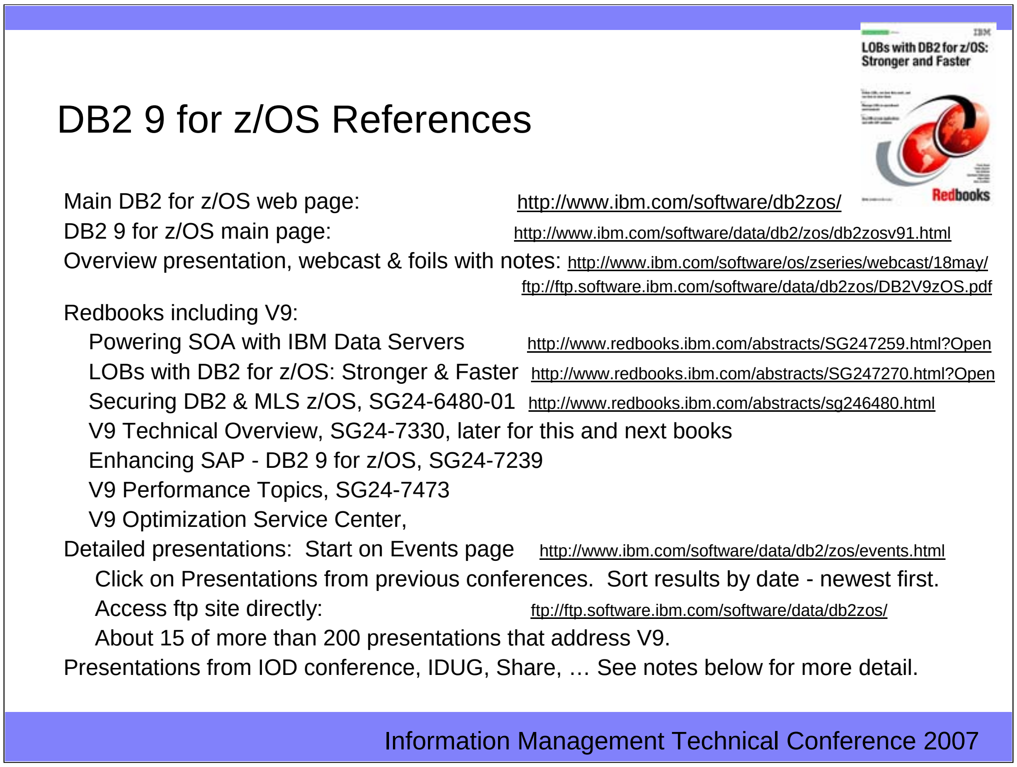
Best Practices of SOA Management
http://www.redbooks.ibm.com/abstracts/redp4233.html?Open

Information Management and SOA
http://www.ibm.com/developerworks/db2/zones/webservices/

DeveloperWorks
http://www.ibm.com/developerworks/

Architecture in Practice: toward SOA
http://www.ibm.com/developerworks/webservices/library/ws-soa-soi/
http://www.ibm.com/developerworks/webservices/library/ws-soa-soi2/
http://www.ibm.com/developerworks/architecture/library/ar-arprac2/

Interview with Jeff Josten



DB2 9 for z/OS References

Main DB2 for z/OS web page: http://www.ibm.com/software/db2zos/
DB2 9 for z/OS main page: http://www.ibm.com/software/data/db2/zos/db2zosv91.html
Overview presentation, webcast & foils with notes: http://www.ibm.com/software/os/zseries/webcast/18may/
ftp://ftp.software.ibm.com/software/data/db2zos/DB2V9zOS.pdf
Redbooks including V9:
Powering SOA with IBM Data Servers http://www.redbooks.ibm.com/abstracts/SG247259.html?Open
LOBs with DB2 for z/OS: Stronger & Faster http://www.redbooks.ibm.com/abstracts/SG247270.html?Open
Securing DB2 & MLS z/OS, SG24-6480-01 http://www.redbooks.ibm.com/abstracts/sg246480.html
V9 Technical Overview, SG24-7330, later for this and next books
Enhancing SAP - DB2 9 for z/OS, SG24-7239
V9 Performance Topics, SG24-7473
V9 Optimization Service Center,
Detailed presentations: Start on Events page http://www.ibm.com/software/data/db2/zos/events.html
Click on Presentations from previous conferences. Sort results by date - newest first.
Access ftp site directly: ftp://ftp.software.ibm.com/software/data/db2zos/
About 15 of more than 200 presentations that address V9.
Presentations from IOD conference, IDUG, Share, … See notes below for more detail.

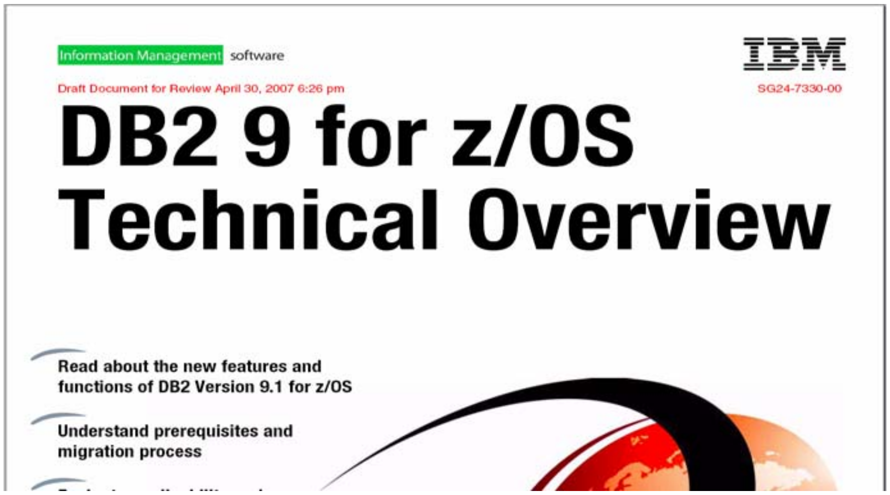
Information Management Technical Conference 2007

Main DB2 for z/OS web page: pointers to most of the following: http://www.ibm.com/software/data/db2/zos/index.html
V9 beta announcement: http://www.ibm.com/common/ssi/fcgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUS206-098
http://www.ibm.com/common/ssi/rep_ca/8/897/ENUS206-098/ENUS206-098.PDF
DB2 9 for z/OS main page: http://www.ibm.com/software/data/db2/zos/db2zosv91.html
Overview presentation, webcast and foils with notes: http://www.ibm.com/software/os/zseries/webcast/18may/
ftp://ftp.software.ibm.com/software/data/db2zos/DB2V9zOS.pdf
Redbooks:
SOA book includes overview of V9 XML http://www.redbooks.ibm.com/abstracts/SG247259.html?Open
LOBs book includes V9 http://www.redbooks.ibm.com/abstracts/SG247270.html?Open
Coming: SG24-6480-01 security, SG24-7330 V9 overview, V9 Performance Topics, V9 Optimization Service Center
Detailed presentations:
Start on the Events page http://www.ibm.com/software/data/db2/zos/events.html
Click on Presentations from previous conferences. Sort results by date - newest first. Some require registration.
http://www.ibm.com/support/docview.wss?rs=64&context=SSEPEK&dc=DA400&q1=presentation&uid=swg27008769&loc=en_US&cs=utf-8&lang=en
http://www.ibm.com/support/docview.wss?rs=64&context=SSEPEK&dc=DA400&q1=presentation&uid=swg27008767&loc=en_US&cs=utf-8&lang=en
http://www.ibm.com/support/docview.wss?rs=64&context=SSEPEK&dc=DA400&q1=presentation&uid=swg27008766&loc=en_US&cs=utf-8&lang=en
http://www.ibm.com/support/docview.wss?rs=64&context=SSEPEK&dc=DA400&q1=presentation&uid=swg27008743&loc=en_US&cs=utf-8&lang=en
Access the ftp site directly: ftp://ftp.software.ibm.com/software/data/db2zos/

IOD2559DB29ClonesLyle.pdf	V9 clone tables
IOD1851DB2v9onlineUtilitiesHartmann.pdf	V9 utilities
IOD1855DB2v9designHartmann.pdf	V9 applicationdesign
IOD1869DB2zOSv9performPreShibamiya.pdf	V9 performance preview
IOD1819PurcellV9.pdf	V9 optimization
IOD1730DB2v9xmlZhang.pdf	V9 XML
IOD1729aDB2v9backuprecoveryTeng.pdf	V9 backup and recovery
IOD1641DB2V9autoQueryTuningFuh.pdf	V9 Optimization Service Center part 1
IOD1642DB2v9autoQueryTuningFuh.pdf	V9 Optimization Service Center part 2
IOD1450aDB2v9SAPHrle.pdf	V9 for ERP and SAP
IOD1438db2v9LOBsWeihrauch.pdf	V9 LOBs
IOD1345DB2zOSmigrationg.pdf	V8 & V9 migration
IOD1166DB2v9zOSbeyondCotner.pdf	V9 overview
DB2V9forzOS.pdf	V9 overview
DB2V9zOS.ppt	V9 overview PowerPoint

IOD conference. There were about 20 presentations there, and most are on the conference web site and on the recently shipped CD.
Sessions from list above are 1166, 1345, 1438, 1450, 1641, 1642, 1729, 1730, 1819, 1851, 1855, 1869, and 2559. 1388 QMF V8 V9
1439 DB2 and SOA
1745 stored procedures
1747 Java stored procedures
2110 V9 not logged table spaces
2461 scalability V8 V9

V9 and V8 migration resources are on the web, and we do have webcasts for some. The primary pointer for resources is the DB2 Events page,
http://www.ibm.com/software/data/db2/zos/events.html



Information Management software

IBM

Draft Document for Review April 30, 2007 6:26 pm

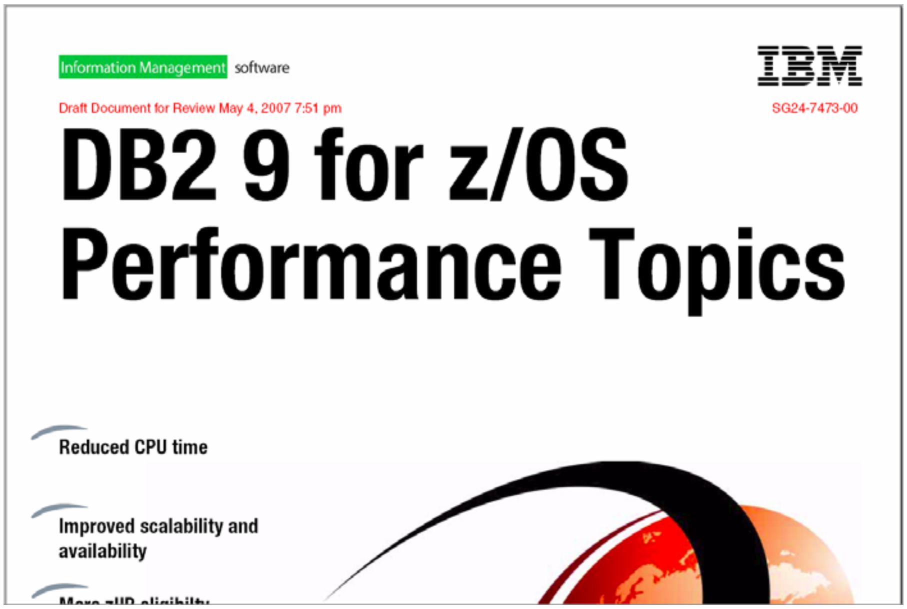
SG24-7330-00

DB2 9 for z/OS
Technical Overview

Read about the new features and functions of DB2 Version 9.1 for z/OS

Understand prerequisites and migration process

This is the upcoming redbook, SG24-7330, describing DB2 9 in detail (roughly 600 pages). Watch for this book in the next month or two.



Information Management software

IBM

Draft Document for Review May 4, 2007 7:51 pm

SG24-7473-00

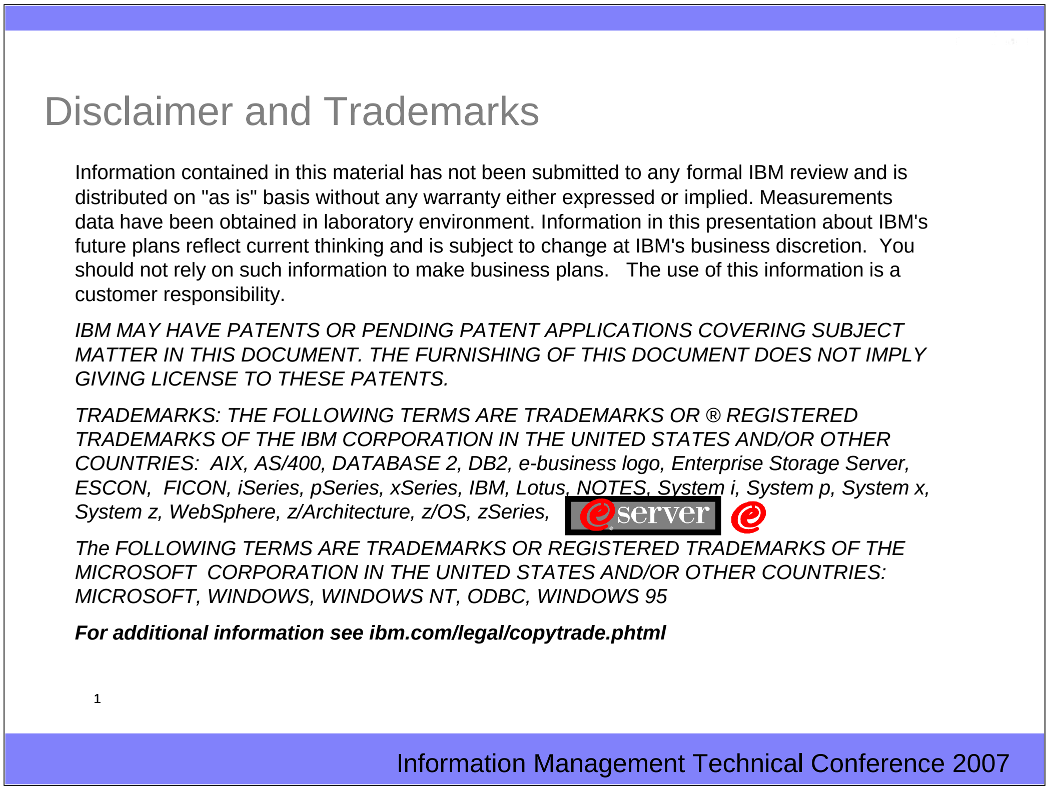
DB2 9 for z/OS Performance Topics

Reduced CPU time

Improved scalability and availability

More zIIP eligibility

This is the upcoming redbook, SG24-7473, describing DB2 9 performance. Watch for this book in the next month or two.



Disclaimer and Trademarks

Information contained in this material has not been submitted to any formal IBM review and is distributed on "as is" basis without any warranty either expressed or implied. Measurements data have been obtained in laboratory environment. Information in this presentation about IBM's future plans reflect current thinking and is subject to change at IBM's business discretion. You should not rely on such information to make business plans.   The use of this information is a customer responsibility.

IBM MAY HAVE PATENTS OR PENDING PATENT APPLICATIONS COVERING SUBJECT MATTER IN THIS DOCUMENT. THE FURNISHING OF THIS DOCUMENT DOES NOT IMPLY GIVING LICENSE TO THESE PATENTS.

TRADEMARKS: THE FOLLOWING TERMS ARE TRADEMARKS OR ® REGISTERED TRADEMARKS OF THE IBM CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES: AIX, AS/400, DATABASE 2, DB2, e-business logo, Enterprise Storage Server, ESCON, FICON, iSeries, pSeries, xSeries, IBM, Lotus, NOTES, System i, System p, System x, System z, WebSphere, z/Architecture, z/OS, zSeries,

The FOLLOWING TERMS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF THE MICROSOFT CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES: MICROSOFT, WINDOWS, WINDOWS NT, ODBC, WINDOWS 95

For additional information see ibm.com/legal/copytrade.phtml

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in the operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.