Achieving Compliance Through Data Governance

Information Management software

Agenda

- Data Governance
- Secure Data Access
- Audit Data Access
- Protect Data Privacy
- Manage Data Growth

Data Governance - Definitions and Goals

- **What is Data Governance**
  - *"Data governance is a quality control discipline for assessing, managing, using, improving, monitoring, maintaining, and protecting organizational information. It is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."*
- **Forrester's view of Data Governance**
  - *"The process by which an organization formalizes the fiduciary duty for the management of data assets critical to its success."*

The top challenge for 43% of CFOs is improving governance, controls, and risk management

CFO Survey:
Current state & future direction,
IBM Business Consulting Services

GOALS OF DATA GOVERNANCE

- Assess the value of data and calculate the probability of risk as part of the decision-making process
  - Data is an asset whose value must constantly be assessed
  - Risk must be forecast by analyzing past losses before mitigation
- The value of data and the probability of risk must both be presented in the decision-making process
- Decisions must be audited and results reported continuously to create operational awareness
- Transparency is its own compliance enabler!

Data Governance - Definitions and Goals

- **Enterprise Data Governance (EDG):** refers to the overall management of the availability, usability, integrity, quality and security of the data employed in an enterprise. It lays the foundation for lower risk and cost, increased profitability and competitive differential

- A sound EDG program includes a defined set of procedures, and a plan to execute those procedures:
  - The initial step in the implementation involves **defining the owners or custodians of the data assets** in the enterprise.
  - A policy must be developed that specifies **who is accountable** for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness, and updating.
  - Processes must be defined concerning how the data is to be stored, archived, backed up, and **protected from mishaps, theft, or attack.**
  - A set of standards and procedures must be developed that defines **how the data is to be used by authorized personnel.**
  - Finally, **a set of controls and audit procedures must be put into place** that ensures ongoing compliance with corporate and government regulations.

Regulatory Compliance

"Today, database security is a lot more challenging than it was a decade ago largely because compliance requirements are more pressing and more complex. Enterprises are dealing with tougher regulatory compliance requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley (SOX) Act, and the Payment Card Industry Data Security Standard (PCI DSS). In addition, since compliance requirements do not offer guidelines, confusion exists around what needs to be done to make databases more secure in order to comply."

- Forrester Research, "A New Role Is Emerging Within IT: Database Security Analyst (DSA)", 4 April 2008

- **Compliance:** The state of being in accordance with Data Governance guidelines, specifications, or legislation or the process of becoming so.

Regulatory Compliance Example

- Payment Card Industry
  - The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard customer information
  - Credit card issuers (Visa, MasterCard, American Express, and others) mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data
  - Severe penalties for non-compliance
  - Synchronicity with other compliance initiatives
  - Compliance viewed by many as competitive advantage

PCI DSS Requirements "The Digital Dozen"

Build and Maintain a Secure Network	
1.	**Install and maintain a firewall configuration to protect cardholder data**
2.	**Do not use vendor-supplied defaults for system passwords and other security parameters**
Protect Cardholder Data	
3.	**Protect stored cardholder data**
4.	**Encrypt transmission of cardholder data sent across open, public networks**
Maintain a Vulnerability Management Program	
5.	**Use and regularly update anti-virus software**
6.	**Develop and maintain secure systems and applications**
Implement Strong Access Control Measures	
7.	**Restrict access to cardholder data by business need-to-know**
8.	**Assign a unique ID to each person with computer access**
9.	**Restrict physical access to cardholder data**
Regularly Monitor and Test Networks	
10.	**Track and monitor all access to network resources and cardholder data**
11.	**Regularly test security systems and processes**
Maintain an Information Security Policy	
12.	**Maintain a policy that addresses information security - Connected Entities and Contracts**

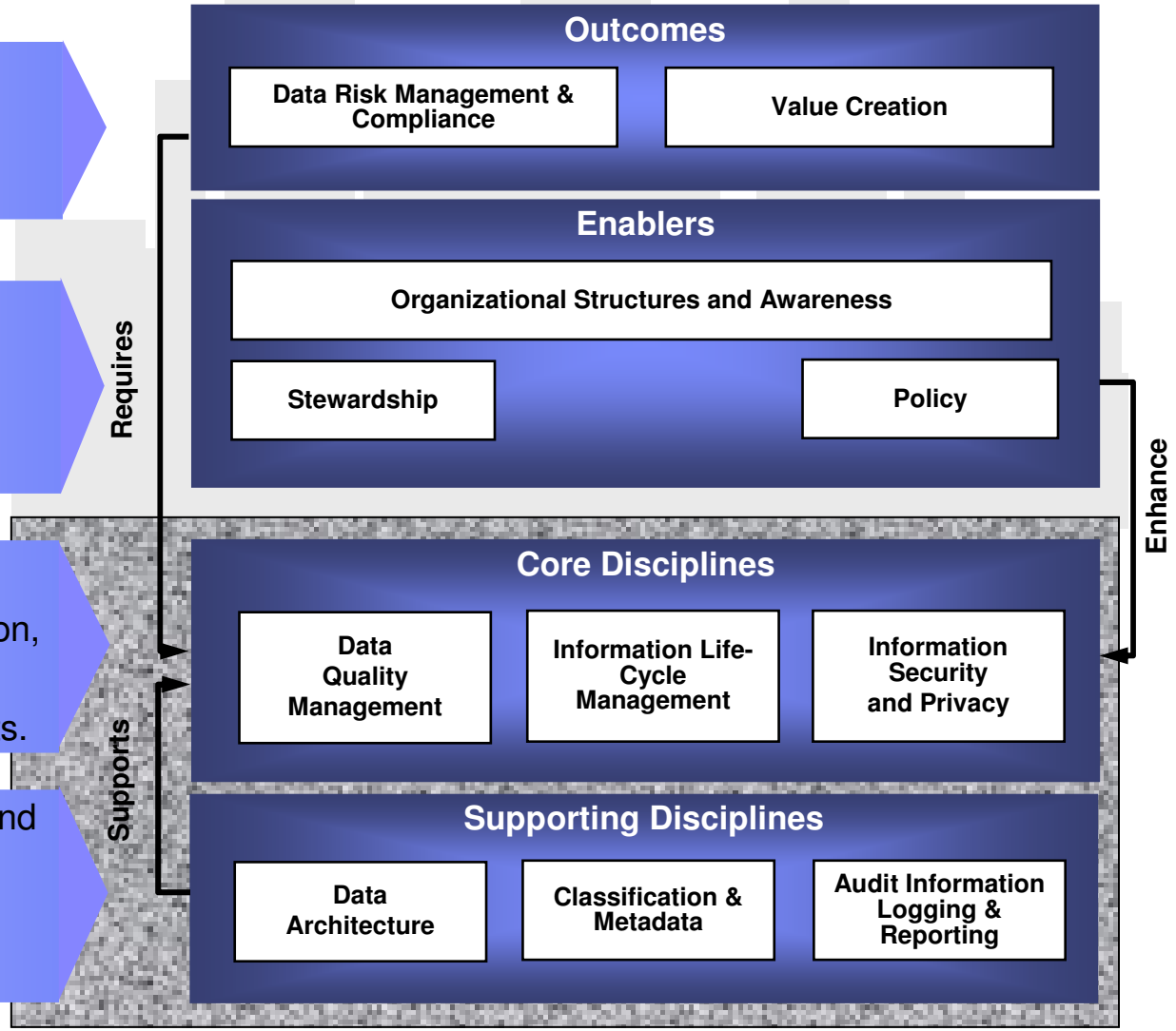
IBM Data Governance - A model for Success

- Lower Risk and Cost
- Increased profitability
- Competitive differential

- IT / Business data responsibilities
- Custodial care of data
- Organizational behaviour

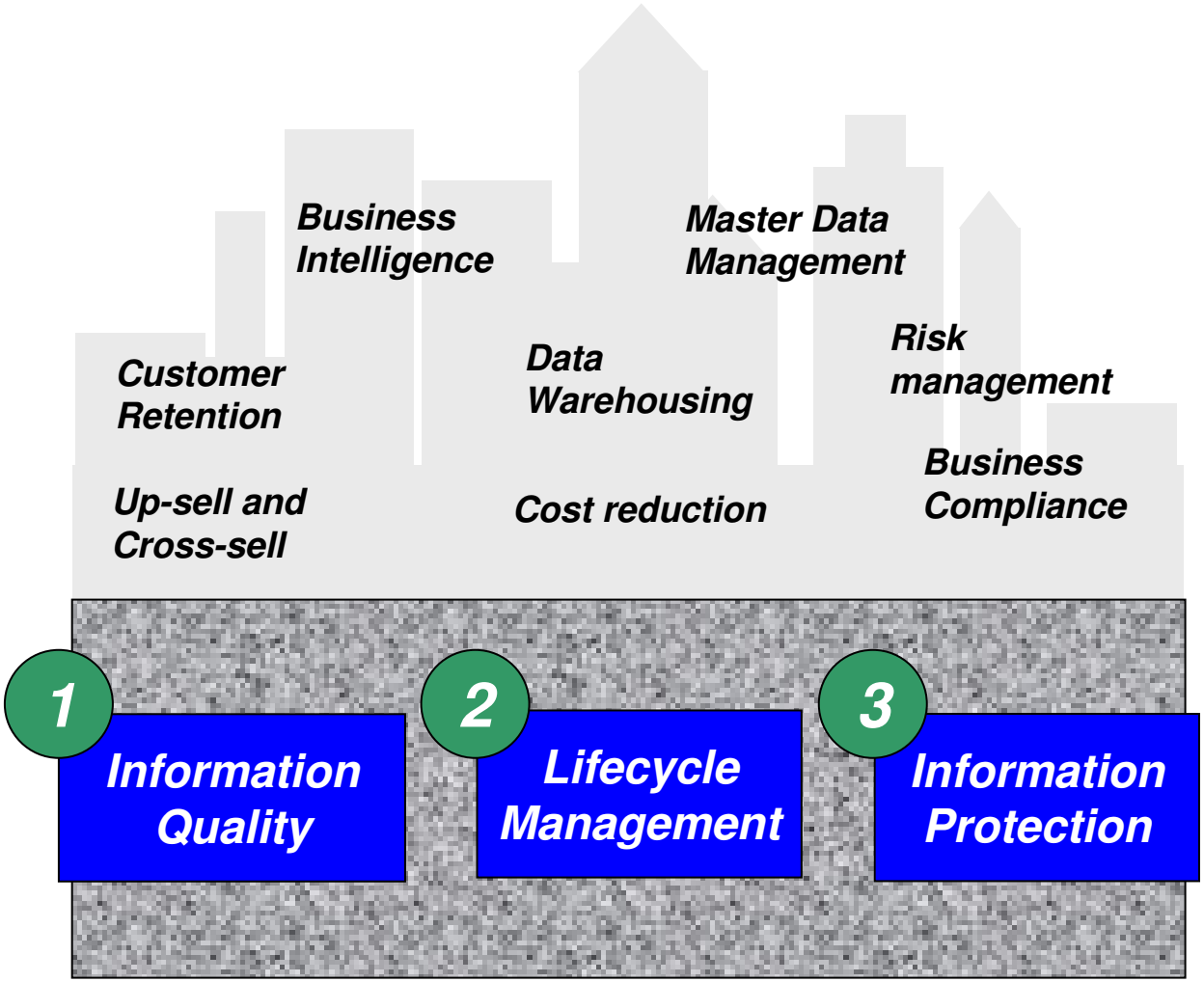
- Quality and integrity of **all** data
- Information collection, use, retention, and deletion
- Mitigate risk and protect data assets.

- Architected design for availability and distribution of data
- Common semantics
- Monitor / measure data value, risk



Foundational disciplines of the IBM Data Governance Council's Capabilities Model

Data Governance "Entry points"



Data Governance underpins and is foundational to your Information Management projects

Information Protection

- *A set of tools for Information Protection that secure access, provide encryption of your data, ensure privacy controls are in place, combining powerful but flexible analysis and reporting tools.*

Secure Data
- Prevent Access
- Restrict Access
- Monitor Access

Ensures that data is secure, available to only those that are authorized and all access monitored

Protect Data Privacy
- Mask Data
- Encrypt Data

De-identification that enables organizations to substitutes sensitive data with realistic and fully functional masked data and encryption of online and off line data sources

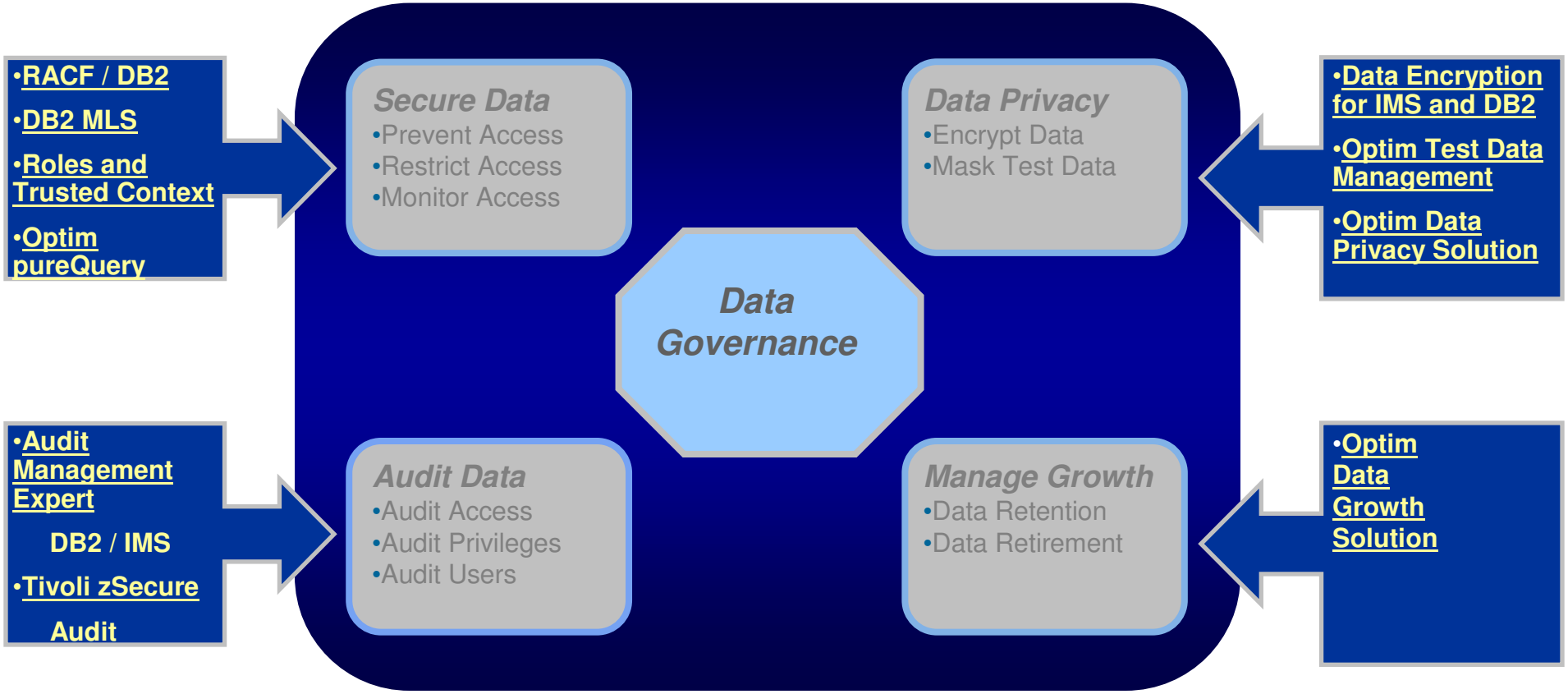
Audit Data
- Audit Access
- Audit Privileges
- Audit Users

Timely data and flexible reporting for use in internal and external auditing activities – The "who, what, when where, how."

"A company with at least 10,000 accounts to protect can spend,
in the first year, as little as $6 per customer account for just data encryption, or as much as $16 per customer account for data encryption, host-based intrusion prevention, and strong security audits combined. Compare [that] with an expenditure of at least $90 per customer account when data is compromised or exposed during a breach,"

**** Garner analyst Avivah Litan***

IBM Data Governance Software for System z




Secure Data Access

Secure Data Access

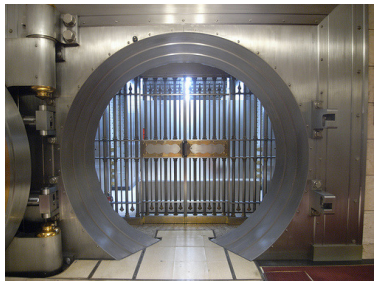
- RACF
  - Centralized administration, authentication and authorization
- DB2 GRANT / REVOKE
  - Access to data via Views and without granting authorities to tables
  - Use package authorization to restrict data access from users
- DB2 v8
  - Multilevel Security with Row Level Granularity
- DB2 v9
  - Roles
  - Trusted Context
    - Restrict data access to secure applications only
  - Auditing

Assign a Unique ID to Each Person

Security Requirements	RACF enforced	DB2 enforced
Render all passwords unreadable during transmission and storage using strong cryptography	RACF encrypts passwords stored in RACF database using one-way encryption protected by z/OS	Can use 256 bit AES encryption (default in 9) to obscure user ID and password during transmission
Control addition, deletion, modification of user IDs	RACF enforced –manages all DB2 IDs	
Require first-time passwords to be change on first use	RACF enforced – ADDUSER (PASSWORD) is always expired	
Immediately revoke access from terminated users	RACF enforced - DELUSER prevents user connecting to DB2	
Disable inactive user IDs every 90 days	RACF enforced - SETROPTS INACTIVE(90)	
Require user passwords to be changed every 90 days	RACF enforced - SETROPTS PASSWORD(INTERVAL(90))	
Require minimum password length to at least 7 characters	RACF enforced - SETROPTS PASSWORD(RULE1(LENGTH(7))	
Require passwords to contain numeric and alphabetic characters	RACF enforced - PASSWORD (RULE1 MIXEDNUM(1:8))	
Limit repeated access attempts after more than six attempts	RACF enforced - SETROPTS PASSWORD(REVOKE(6))	
Force a new logon after connection is idle for more than 15 minutes		DB2 enforced - IDLE THREAD TIMEOUT(IDTHTOIN) subsystem parameter
Require user ID authentication for any access to any object containing sensitive data		DB2 enforced – An authenticated user ID is always associated with a DB2 process

Optim pureQuery for More Secure Applications

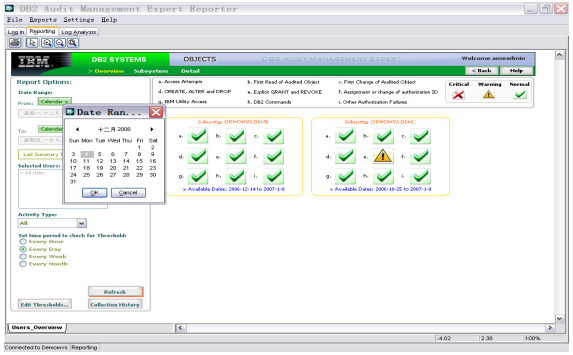
- SQL Injection is a common vulnerability to sensitive data
  - Use static SQL when accessing any sensitive data
  - SQL injection happens because the database cannot effectively distinguish between static portion of the SQL statement and the user input
  - An SQL statement is inserted into pre-defined SQL via user input
    - Another query or data modification or database command
  - Optim pureQuery can help prevent SQL injection by turning dynamic SQL into static SQL
    - Grant access to data through a static plan
    - Predictable access paths for improved performance
    - Enhanced audit capability




Audit Data Access

Audit Management Expert

- **Helps auditors answer:**
  - Who, What, Where, Why, When, How
- **Centralizes the audit data**
  - Pulls together disparate data sources from all the systems into a central repository
- **Automates auditing process**
  - Eliminates all home grown processes
- **Creates segregation of duties**
  - Gives auditors the business activity collected without being reliant on the technical personnel they need to monitor
- **Flexible Reporting**
  - Drill down from overview to detail for forensic analysis



Audit Management Expert

- Supports internal and external auditors in the collection and reporting of DB2 audit data
- Does not require auditors to be DB2 users within the monitored DB2 systems
- Does not require the auditors to log on to the operating system where the monitored system is running
- Does not require extensive interaction between the auditor and the system support personnel (DBA / Systems Administrator)
- Auditors will not be able to directly manipulate any DB2 resources
- Provides complete visibility of all auditable objects to an administrator level user
- Provides controls for limiting visibility to auditors of auditable objects

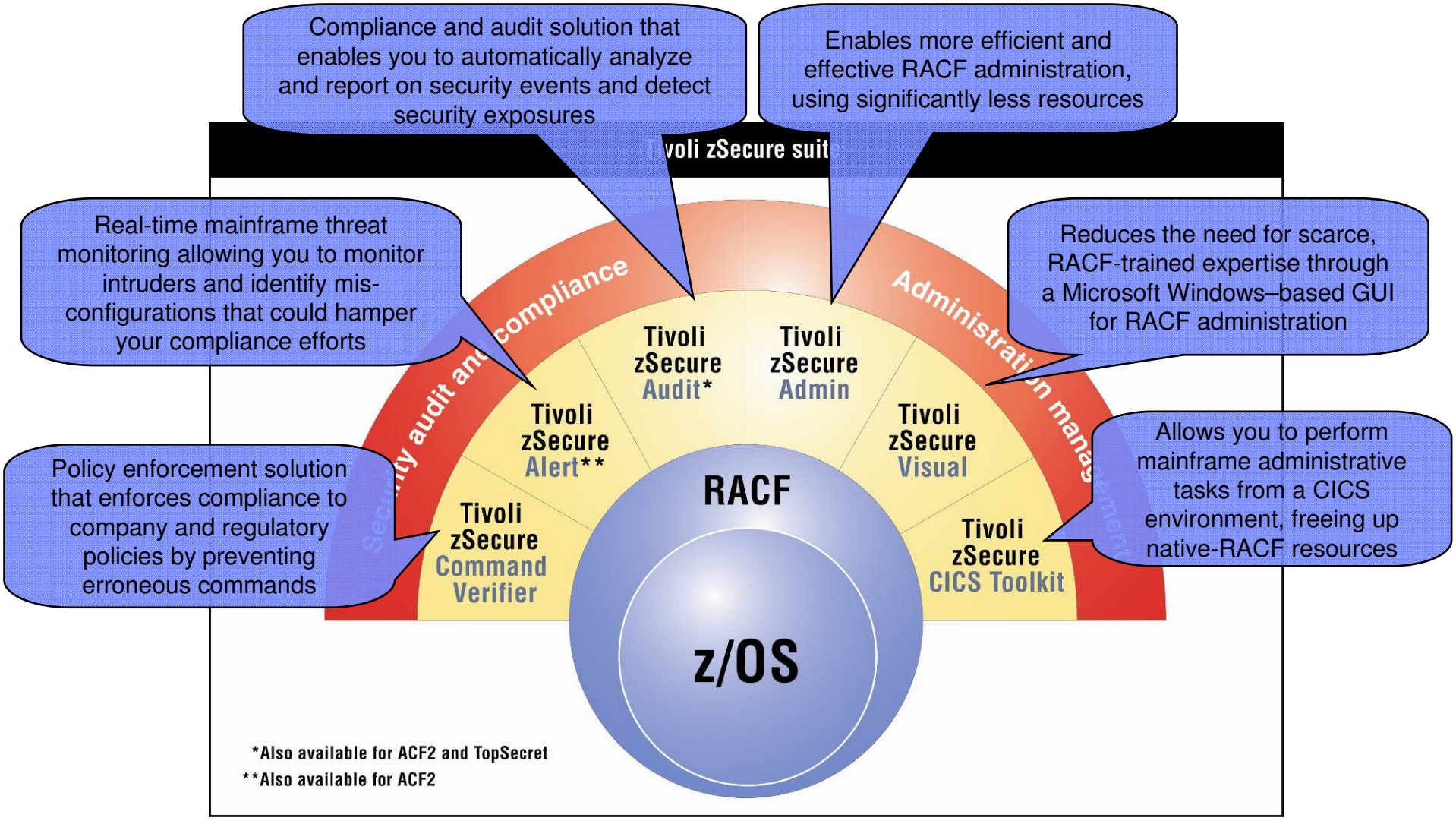
Sources of Auditing Information on DB2 z/OS

- DB2 z/OS IFI (Audit Trace Records)
  - Access attempts denied due to inadequate authorization
  - Explicit GRANT and REVOKE
  - CREATE, ALTER, and DROP operations against audited tables
  - First change of audited object (SQL INSERT, UPDATE, and DELETE)
  - First read of audited object (SQL SELECT)
  - Bind time information about SQL statements that involve audited objects
  - Assignment or change of authorization ID
  - Utilities
  - DB2 commands
- DB2 Recovery Log for UPDATE, INSERT, AND DELETE activity
  - DSN1LOGP (offline utility)
  - DB2 Log Analysis Tool (separately priced product)

DB2 Audit Management Expert

- Auditors will be able to Access:
  - SELECT, INSERT, UPDATE, and DELETE activity by user or by object
    - All DML instead of first read or first update only
    - No need to ALTER tables to audit read and update activity
    - SQL Text and Host Variable value for each statement
    - Row count that SQL statement affects
    - DB2 Catalog Objects can now be audited for SQL read/update
    - Details of UPDATE activity
  - CREATE, ALTER, and DROP operations against an audited object
  - Explicit GRANT and REVOKE operations
  - Utility access to an audited object
  - DB2 commands entered
  - Assignment or modification of an authorization ID
  - Authorization failures

IBM Tivoli Security Management for z/OS

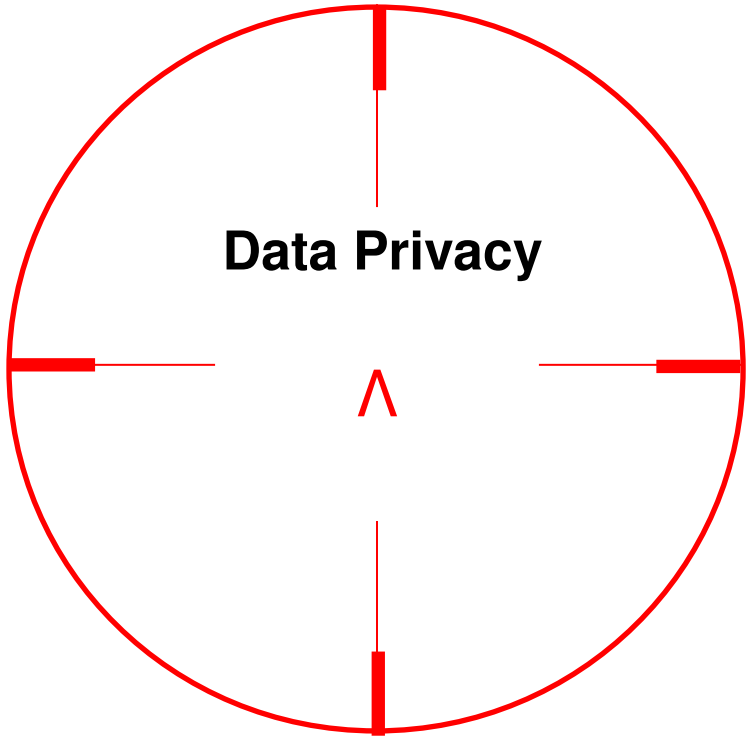


Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Tivoli Security Information and Event Management

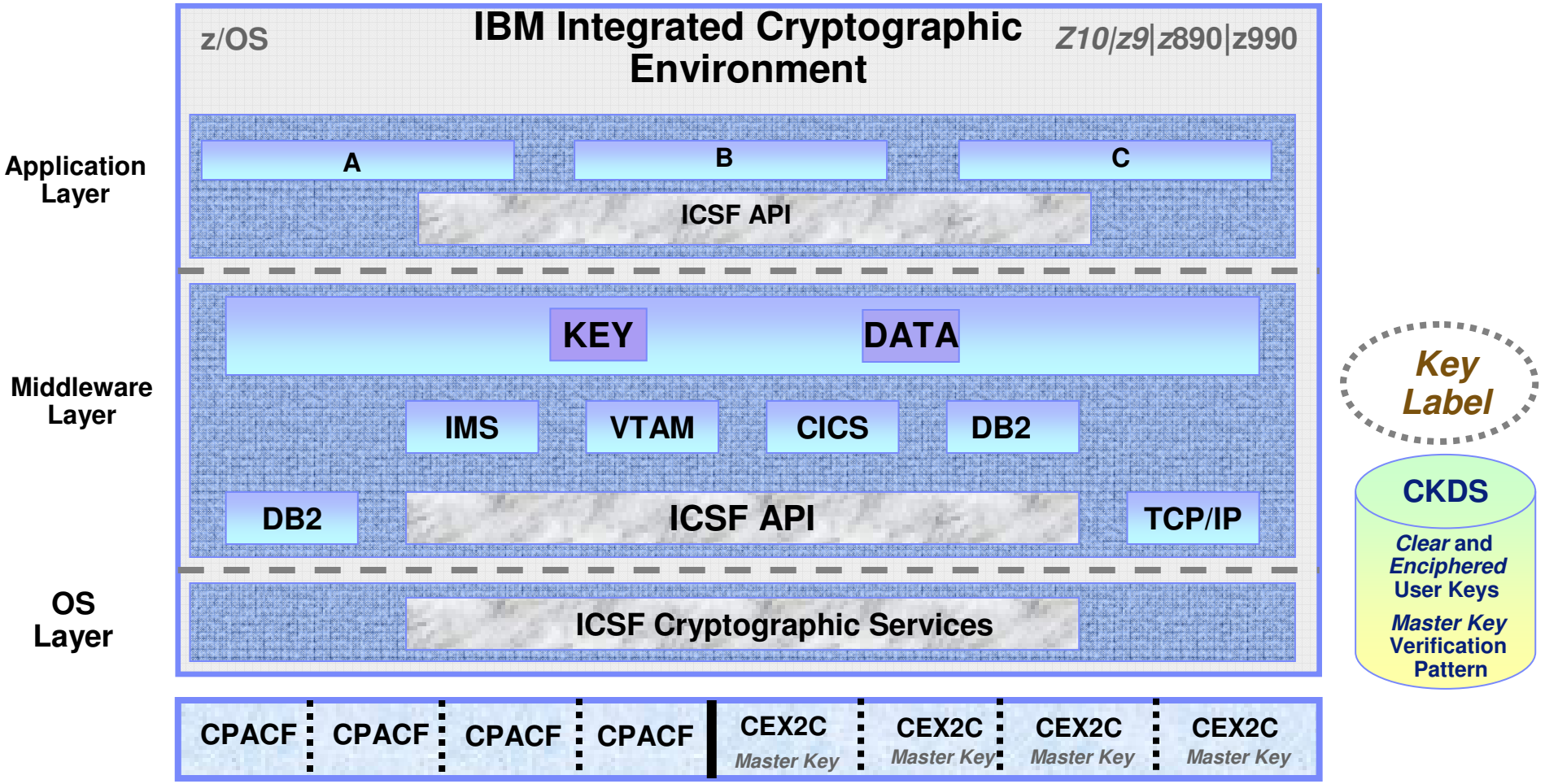
Compliance Reporting Across the Enterprise

- Critical data sources mapped to regulatory specific reports
- Are information controls being enforced?
- Understand who is accessing information
- Identify any abnormal data access patterns
- Monitor security posture of infrastructure supporting information storage and collaboration
- Can you provide proof to internal and external auditors?


Data Privacy

Encrypt Sensitive Data

- System z Encryption
  - DB2 for z/OS Column Level (Built-in Function) Encryption
  - IBM Data Encryption for IMS and DB2 Tool
    - Protect sensitive data from intruder gaining access to datasets containing sensitive data making it unreadable
    - Separate from the native operating systems mechanisms
    - Image Copy and Archive Log recovery assets also protected
  - IBM z/OS Encryption Facility can be used to protect sequential data and safely share with outside partners using OpenPGP
  - IBM Tape Encryption Solutions
    - Protects logs and traces containing sensitive data
    - Encrypts data at near native tape drive speeds on the tape device itself after compressing the data
  - IBM Disk Encryption Solutions
    - Full disk encryption that provides seamless data encryption of all data at rest within the DS8000



CP Assist for Cryptographic Functions

- Problem State Instructions
- Clear Keys Only
- DES/TDES Encryption
- AES (128 Bit)
- SHA-1 (256 on z9)

Crypto Express 2 Coprocessor

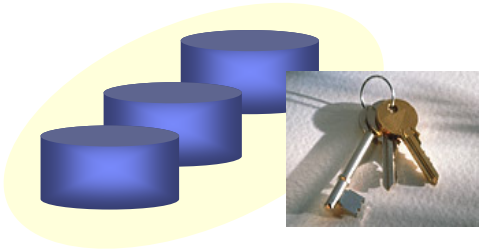
- ICSF Access Only (Key 0)
- Master Key Stored Within Boundary of Crypto Express 2 Feature
- Secure Key DES/TDES Encryption
- SSL Accelerator
- Tamper Resistant

DB2 v8 Built-in Functions for Data Encryption

- Standard feature of DB2 v8
- Addresses Open Standards requirements
- Built-in encryption primitives for the application programmer
- Requires application changes and column definition changes
- Encryption at the column or cell (value) level
- Encryption key constructed from encryption password
- Password specified by user for column or cell
- Password hint can be provided in case password is forgotten
- Clear key or secure key support
- DB2 v8 requires zSeries processor

IBM Data Encryption for IMS and DB2 Databases

- All supported versions of DB2
- Pre-coded EDITPROC routines
- Encryption / decryption occurs at the row level
- Same or separate EDITPROC routine can be selected for each table
- Exploits z/OS Integrated Cryptographic Service Facility (ICSF)
- Exploits zSeries Cryptographic Hardware
- Clear key or secure key support
- Requires no changes to applications
- No password (key label) coding
- Fast implementation



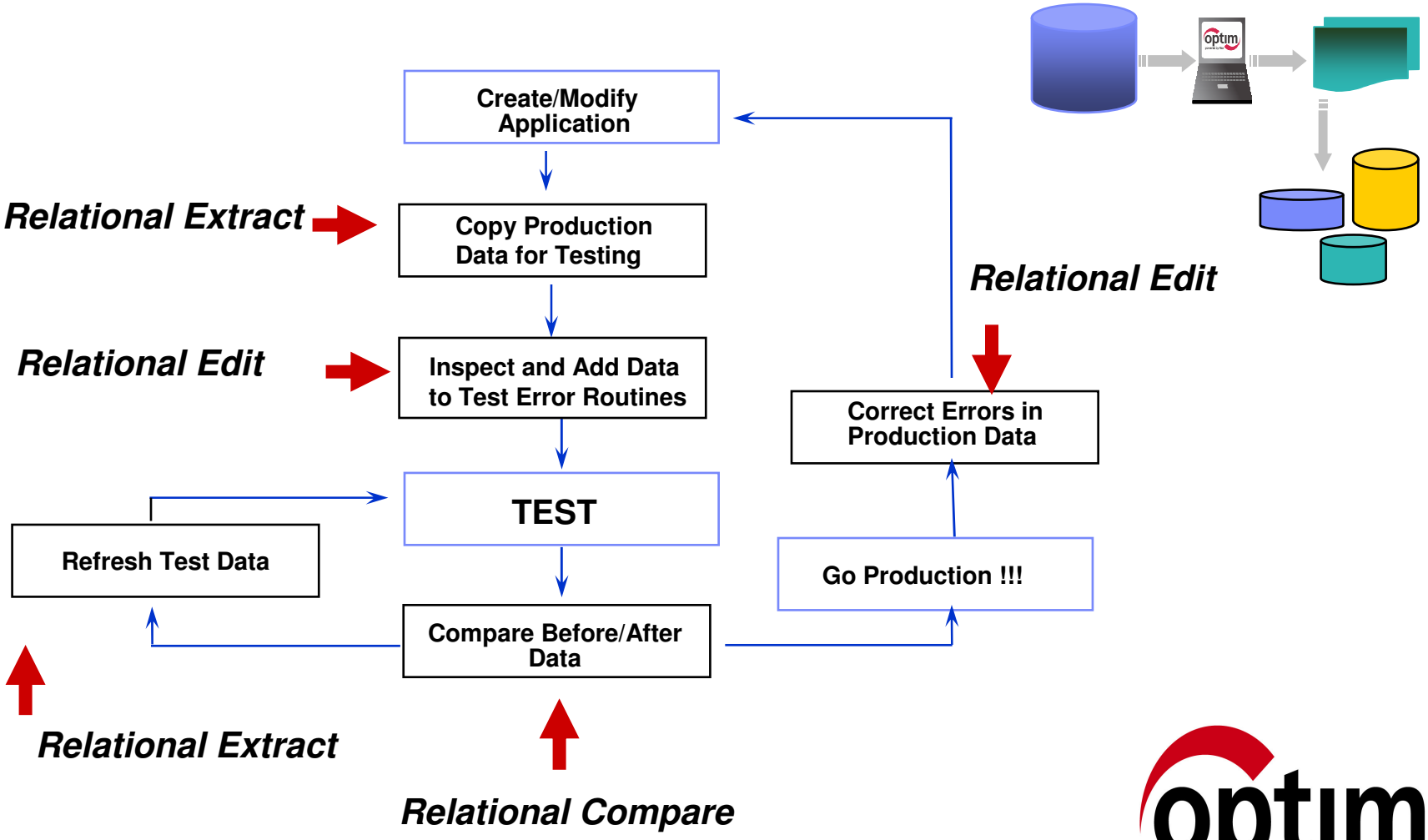
Comparison of DB2 Encryption Options

Feature	DB2 v8 Encryption	DB2 Encryption Tool
Clear key and secure key encryption	Yes	Yes
Requires cryptographic coprocessor	Yes	Yes
DB2 version support	DB2 v8 only	DB2 v7 and DB2 v8
Implementation	SQL - Built-in Functions	EDITPROC Routines
Encryption granularity	Column	Entire row
Structural changes required	Yes	Yes
Application changes required	Yes	No
Encrypts data in indexes	Yes	No
Additional query performance degradation possible	Yes	No
Log data encrypted	Yes	Yes
Image copy data encrypted	Yes	Yes
Data encrypted or decrypted during LOAD / UNLOAD / REORG	No	Yes

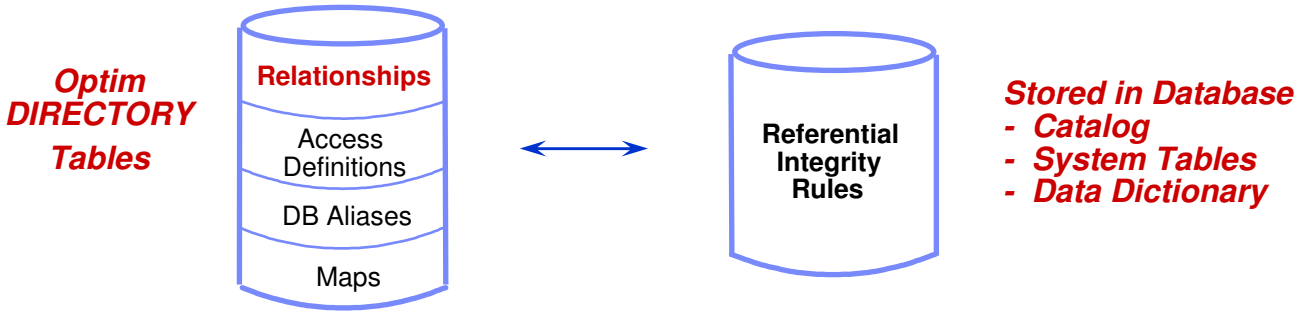
Test Data

- Create test data using subsets of operational data with Optim Test Data Management
- Disguise sensitive data
  - Testing with production data
  - Warehousing with operational data feeds
  - Offshore development and support activities
  - Prevent sensitive data from being exposed in DB2 indexes, DB2 logs, and DB2 traces
  - Use OPTIM Data Privacy masking functions to obscure sensitive data

Optim Test Data Management

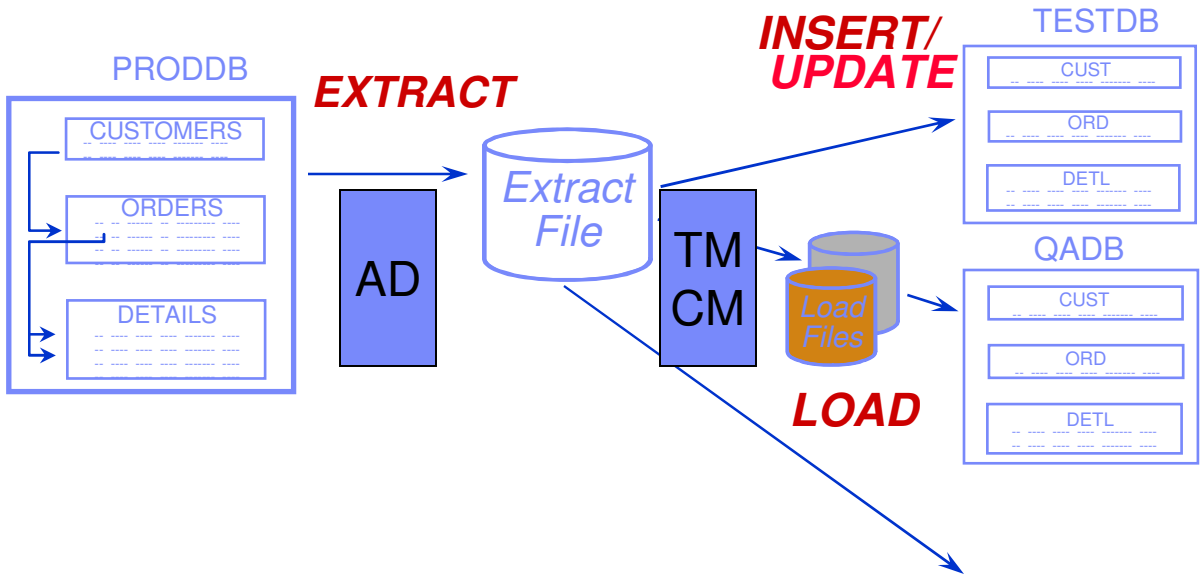


The Optim Directory

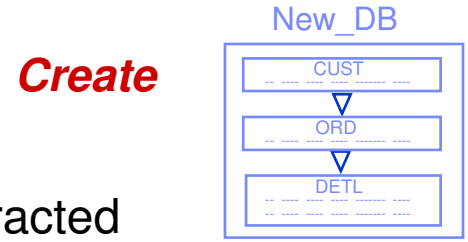


- Optim Directory
  - Supplements information stored in the database
  - Maintains product definitions and tracks processing
  - Stores database connection information (DB Aliases)
  - Stores user-defined relationships

Optim TDM Relational Extract Facility

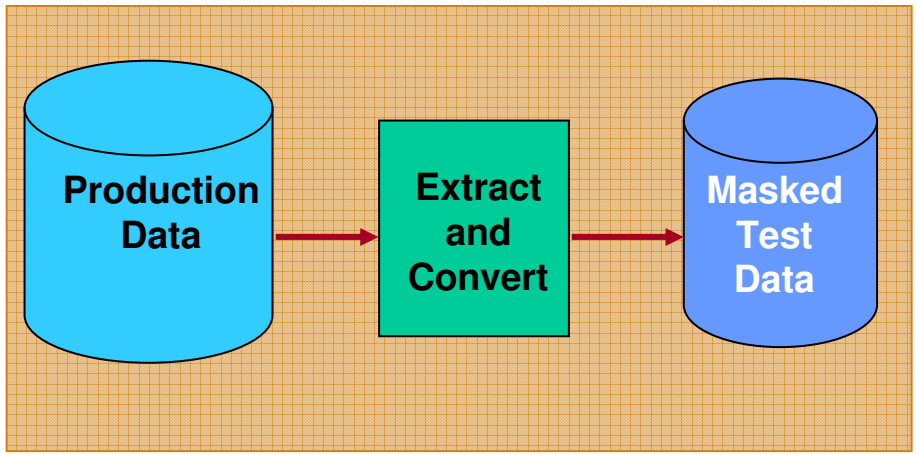


- Creating and maintaining test data bases
- Migrating data
- The data and/or the object metadata can be extracted



Optim Data Privacy Solution

De-Identify test data



During Extract Process

Or

Standalone Convert Process

Or

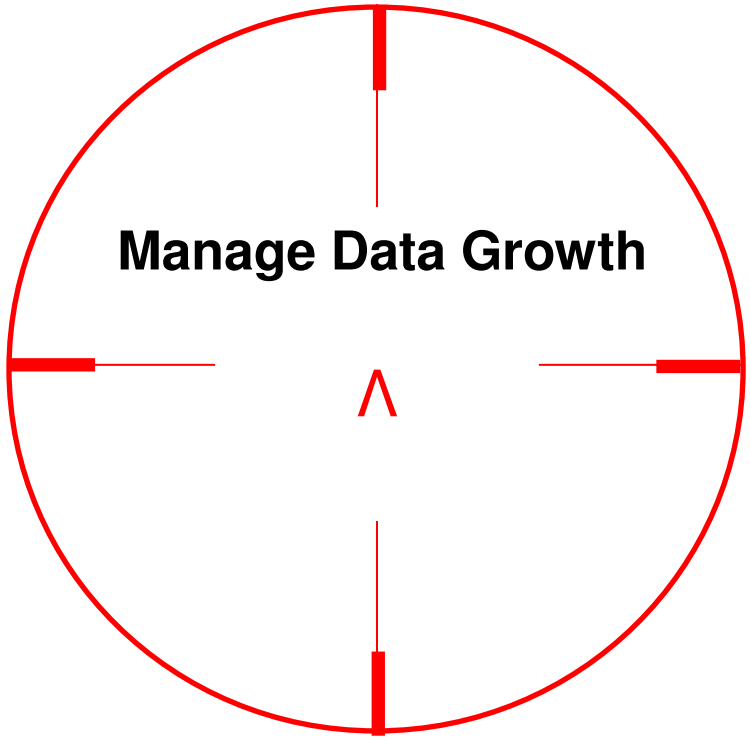
During Insert/Load Process

Transform or Replace sensitive data using

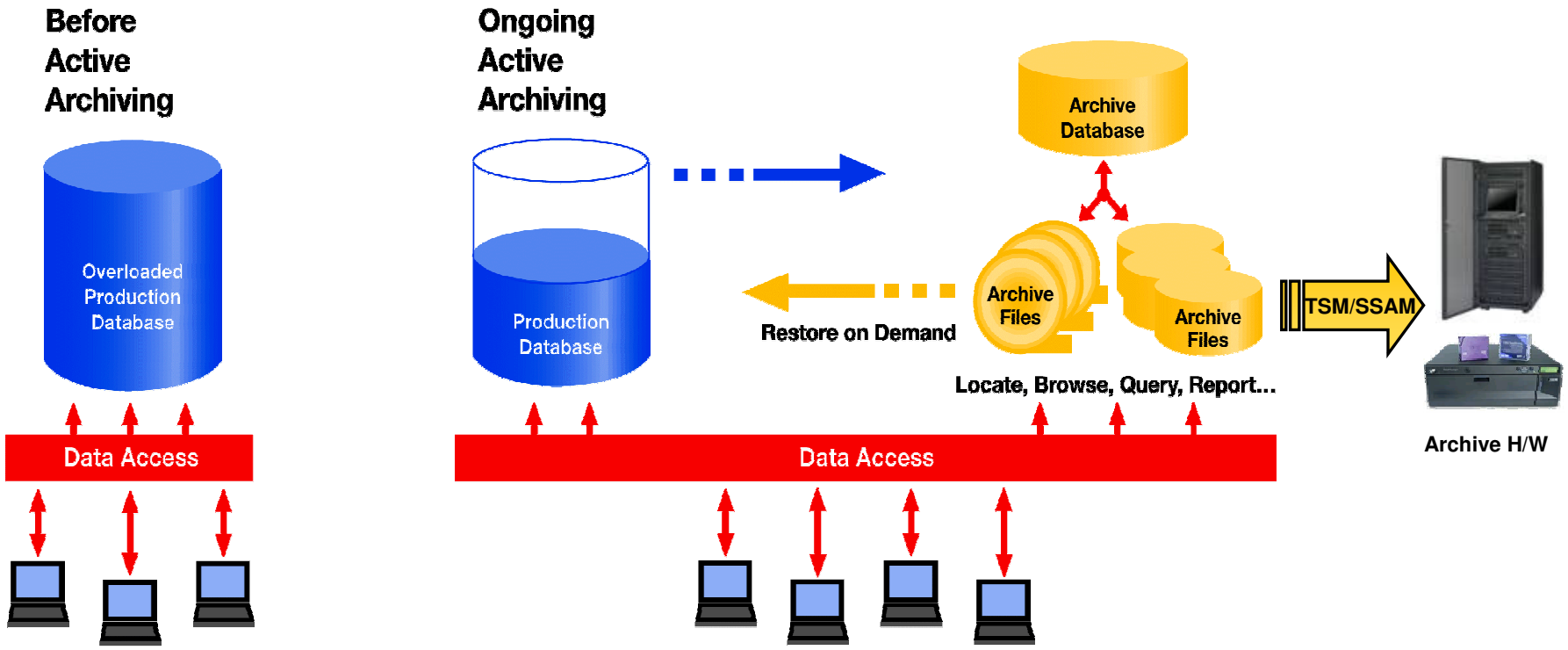
- Standard mapping rules: Literals, Special Registers, Expressions, Default Values, Look-up tables Look-up tables, SSN, Credit Card Number
- Complex mapping rules: User exits

Optim Data Privacy Solution

- Protect sensitive data when it is used for other purposes:
  - Test; Warehouse; Offshore
- Remove, mask or transform elements that could be used to identify an individual
  - Name, telephone, bank account, taxpayer identifier…
- Masked or transformed data must be appropriate to the context
  - Consistent formatting (alpha to alpha)
  - Within permissible range of values
  - Context and application aware
  - Maintain referential integrity

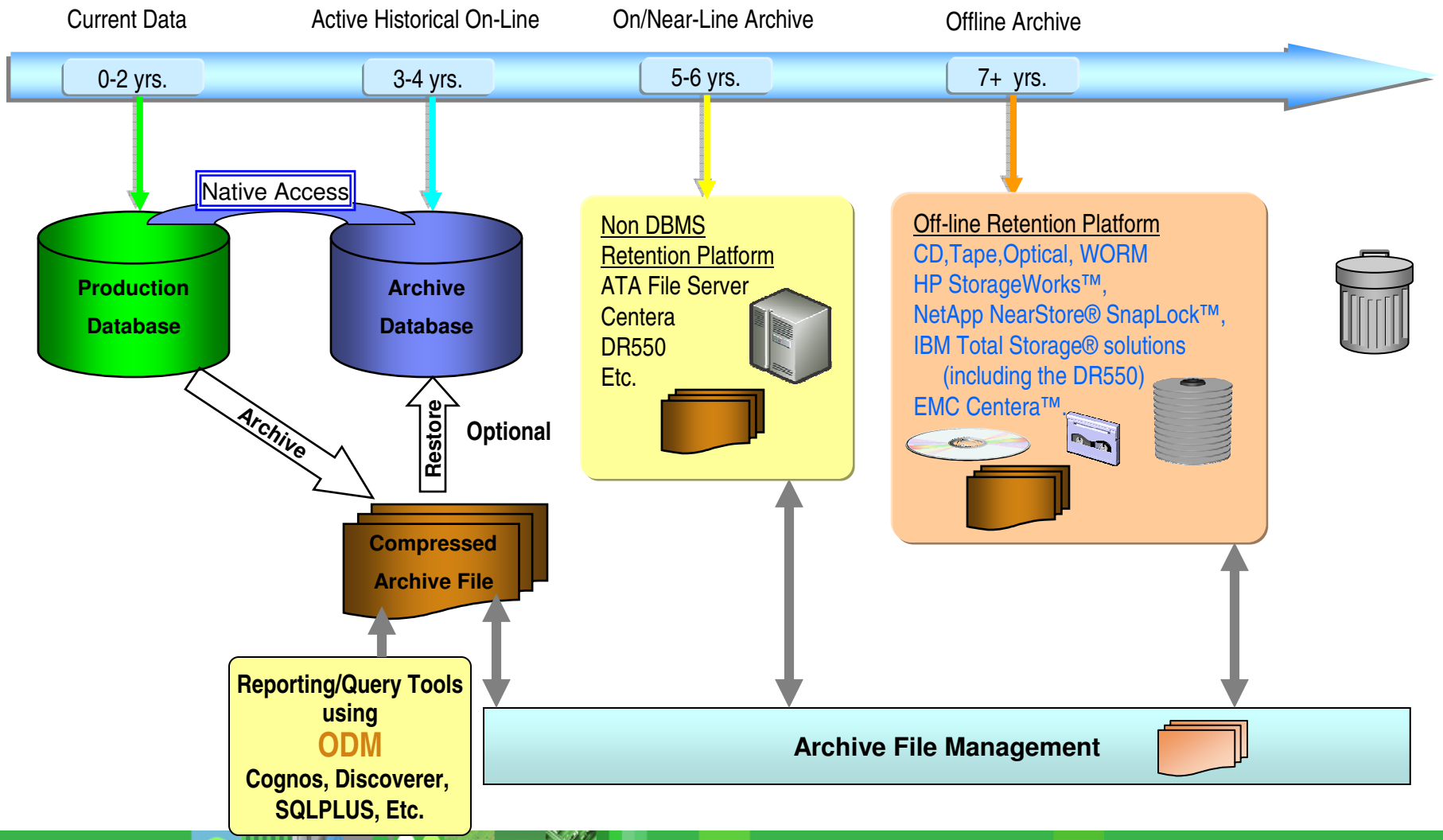

Manage Data Growth

Data Retention and Archiving

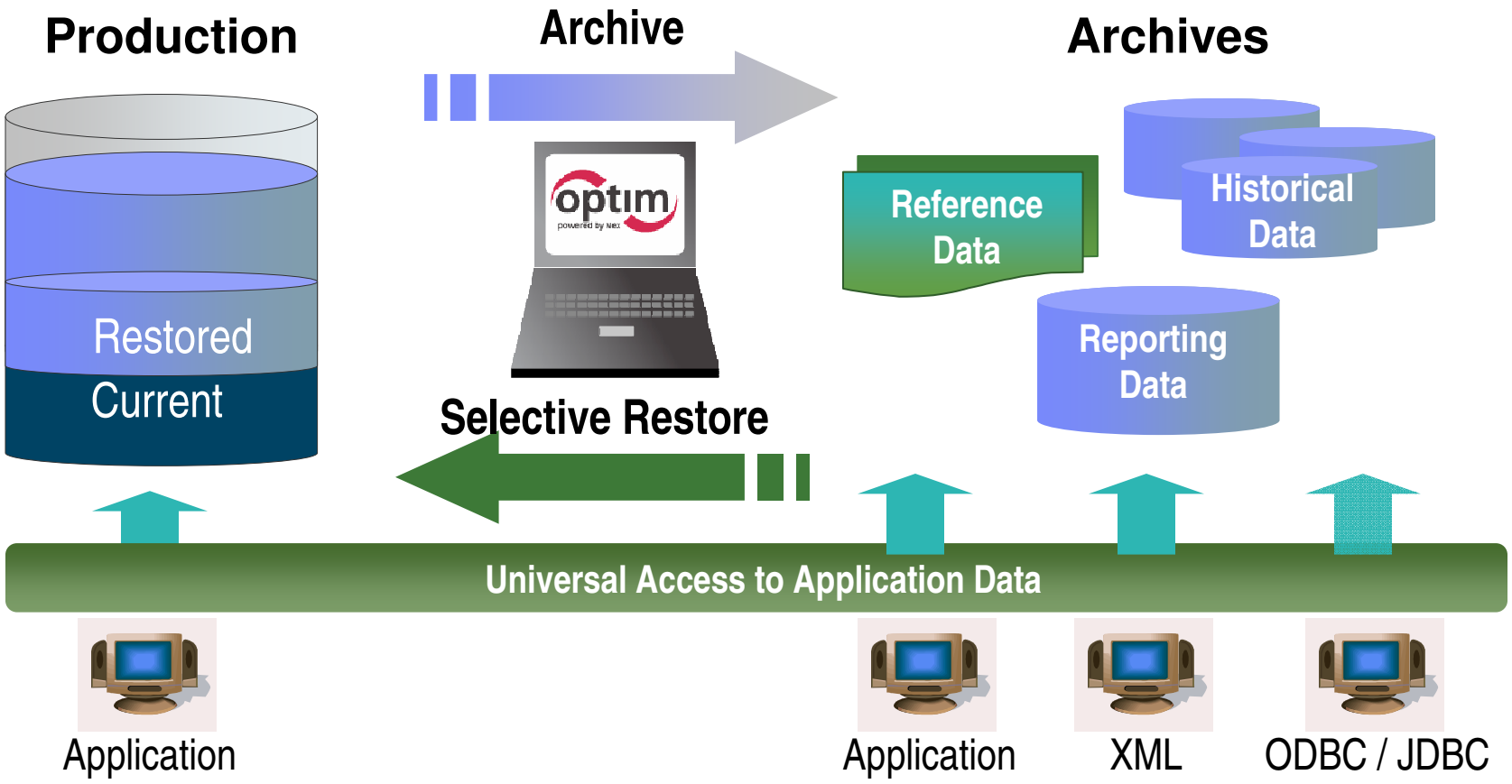


- Complete Business Object – capture all related data objects for complete data retention
- Provides historical reference snapshot of business activity
- Storage device independence enables Information Lifecycle Management
- Immutable file format enables data retention compliance

Information Lifecycle



Optim Data Growth Solution

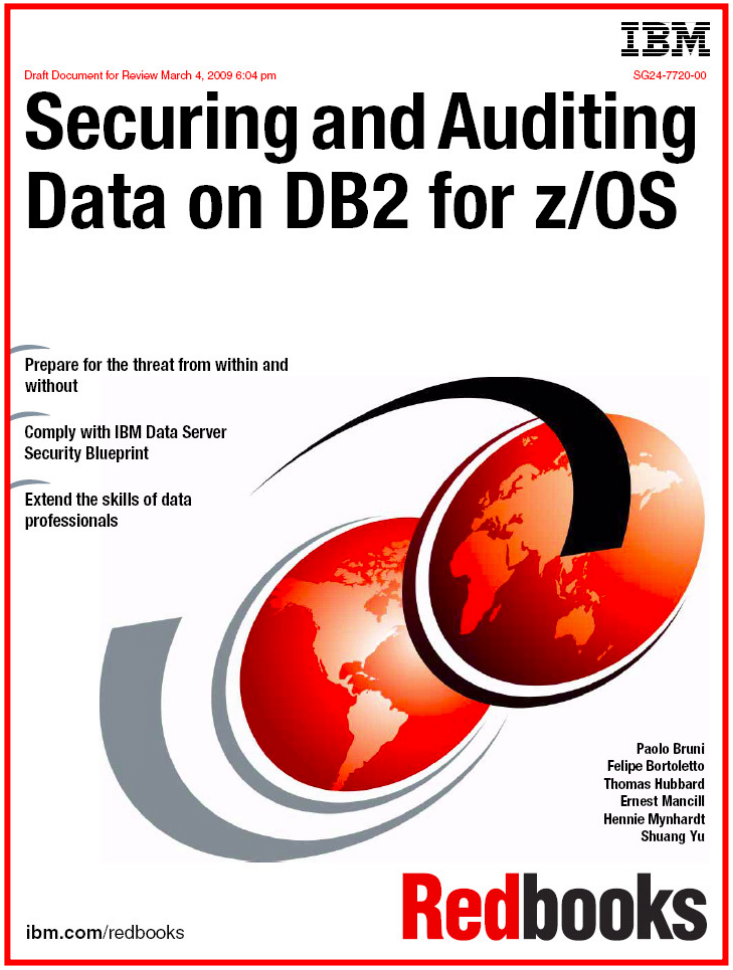


- Complete Business Object provides historical reference snapshot of business activity
- Immutable file format enables data retention compliance

PCI - IBM Compliance Solution

- **Requirement 3: Protect Stored Data**
  - Encryption - IBM Data Encryption for IMS and DB2 Databases
  - Retention - Optim Data Growth Solution
- **Requirement 6: Develop and Maintain Secure Systems and Applications**
  - Secure applications - Optim pureQuery
  - Separate production and test environments - Optim Test Data Management / Optim Data Privacy Solution
- **Requirement 7: Restrict Access to Data by Business "Need to Know"**
  - Access Control - RACF / DB2 Engine Security
- **Requirement 10: Track and Monitor All Access to Data**
  - Auditing and Reporting - Audit Management Expert / Tivoli zSecure Suite

Redbook on Securing Data on DB2 for z/OS: SG24 - 7720



Summary

- **Take Back Control with IBM Data Governance solutions**
  - Transform your information from a Liability into your most strategic, valuable Asset
  - Help manage business risk by enforcing security, audit and privacy controls
  - Lower operational costs by optimizing data management, retention and archiving

- **Hardware and Software**
  - zSeries is the ultimate platform to govern your enterprise data
  - z/OS and System z provide the strongest encryption, authentication, access controls, and auditing features in the industry
  - Information Management provides the most complete end-to-end Data Governance software solutions


Thank
You