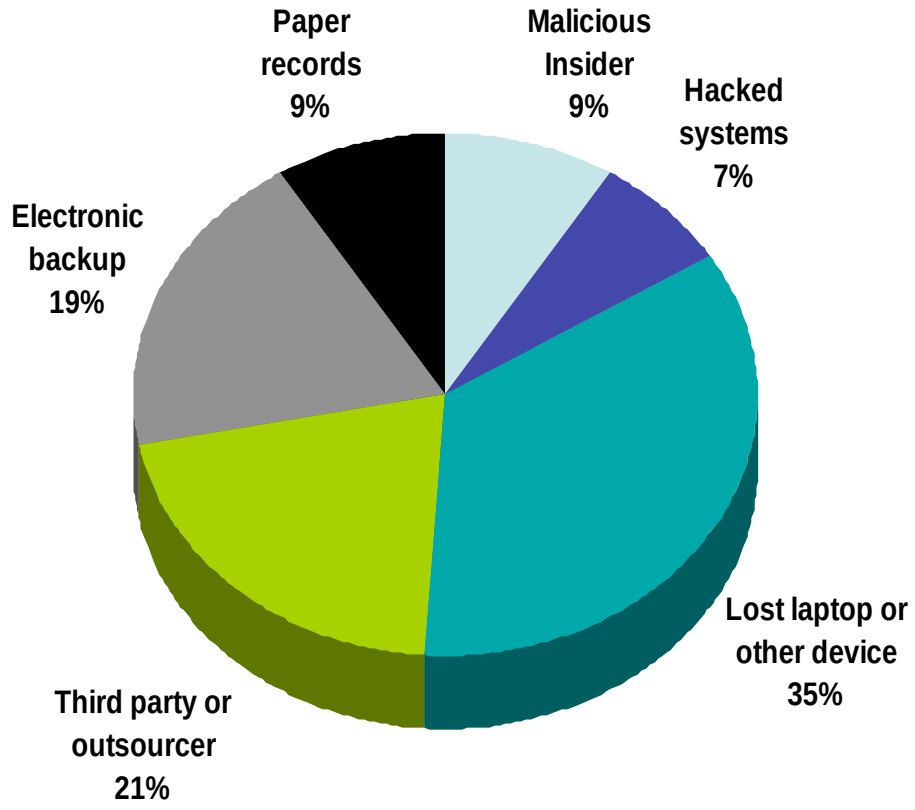
Data Privacy - Protection from Trusted Users

Scott Smith
Compuware Field Technical Specialist
September 19, 2007

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Data Privacy

Most Common Data Losses



Ponemon Institute

2006 Annual Study: Cost of a Data Breach

Data Privacy

Most Common Data Losses

"It is a serious mistake to think that mainframe applications are safe by default. They are not….. Enterprises should not experience a false sense of security simply because their mission-critical applications run on mainframes. Yet, they are often defenseless against insiders equipped with in - depth knowledge of the applications' logic and security policies — those using legitimate means to ill-exploit the system. ***Most attacks on legacies come from inside the enterprises, committed by their own employees... Applications should be protected from the inside out."***

Joseph Feiman, Gartner Research, September 29 2006

Implementing Security for Mainframe Legacy Applications - Worth the Investment

Data Privacy

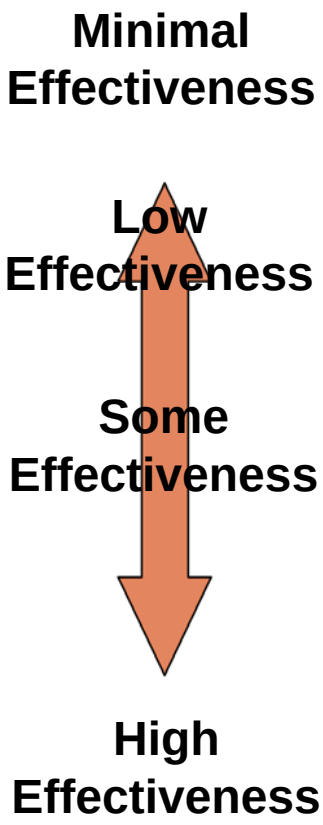
Environmental Differences for data use

Production Region	Test Region
Live customer/account information	Live customer/account information
Access through applications with role based information accesses	Direct access to the raw data
Trained access to employees through policies and agreements	Wider exposure to non-employees or employees across the world
Usage of data monitored and traced for compliance	Higher potential for unauthorized viewing and usage
Successful usage requires 'live' data	Successful testing does not require 'live' data
Region security mature and robust, through tools and processes	Region security not as robust as production

Test Data Privacy

How we see it being addressed

- Signing non-disclosure agreements
- Restricting security access to sensitive/ confidential data
- Applying minimal “de-identifying” rules
- Implementing a complete data disguise solution with processes and procedures



Test Data Privacy

Internal Challenges

Organizational	Political	Technical
• Defining ownership of the data • Disguise enforcement • Defining disguise standards • Business process management • Designing and implementing corporate disguise policies and procedures	• Communication and agreement between different application groups • Conflicts of interest • External influences • Interpretation of the compliance regulations	• Variety of platforms • Variety of data types • Data complexity • Maintain shared relationships between multiple environments • Coordination of physical implementation

Test Data Privacy

Requirements for Success

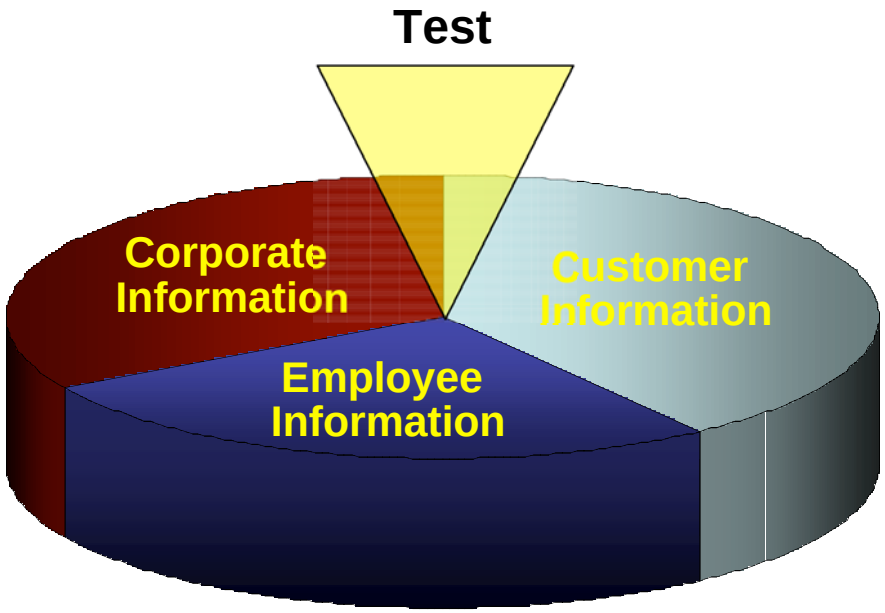
- **Process**
  - A clear strategy backed up by a methodology that serves as a roadmap or blueprint for an enterprise-wide data privacy initiative
- **Technology**
  - Tools that can deliver quality data that meets the integrity, consistency and usability demands of your data privacy requirements
- **Expertise**
  - The knowledge and experience to effectively manage the process and drive the technology to implement data privacy assurance in the application testing environment

Test Data Privacy
Leadership

- **Provide Products, Processes and People to disguise and generate data used for:**
  - Application testing
  - Data exchange
  - Internal reporting
  - Offshore / outsourced development
  - Departmental data processing

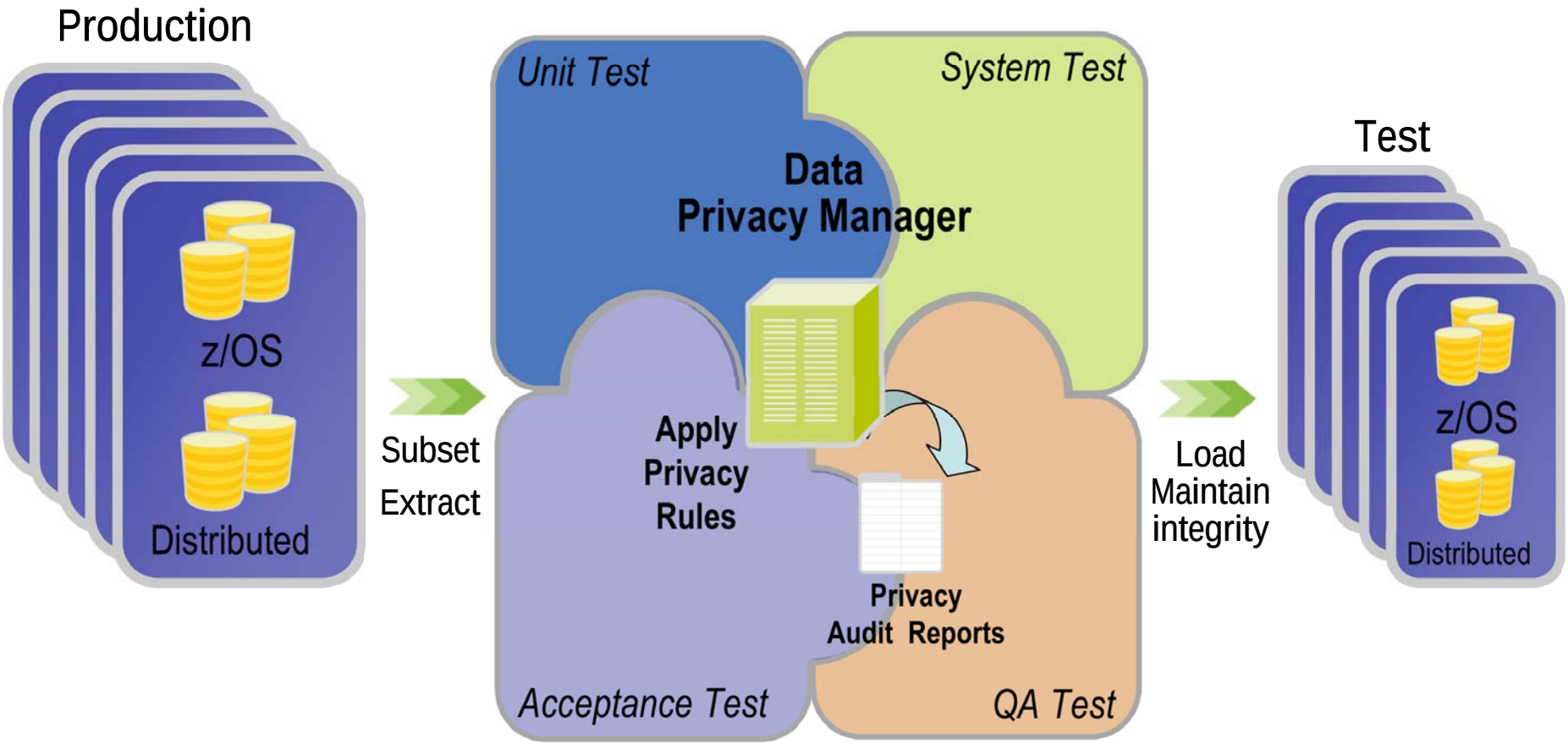
Test Data Privacy

Delivery



- **Protect personal/sensitive data while maintaining:**
  - Data Integrity across application(s)
  - Consistency, regardless of data source, and repeatability
  - Usability, test data should be valid and meaningful

Test Data Privacy
Solution



Test Data Privacy

Process: Methodology

Analyze – Understand each application's sensitive information

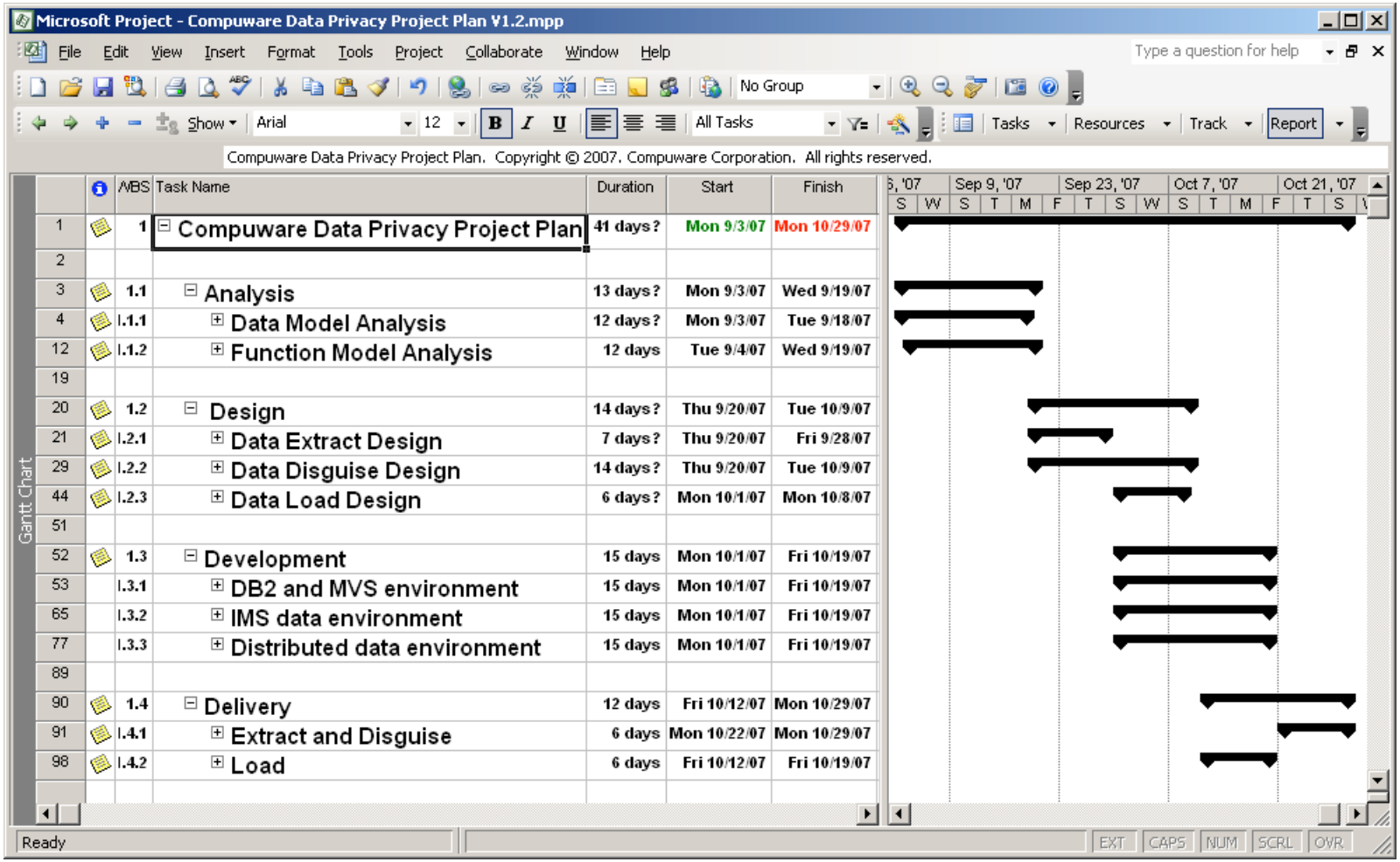
Design – Define strategies for disguising test data

Develop – Build the processes to disguise test data

Deliver – Deploy and maintain data protection processes

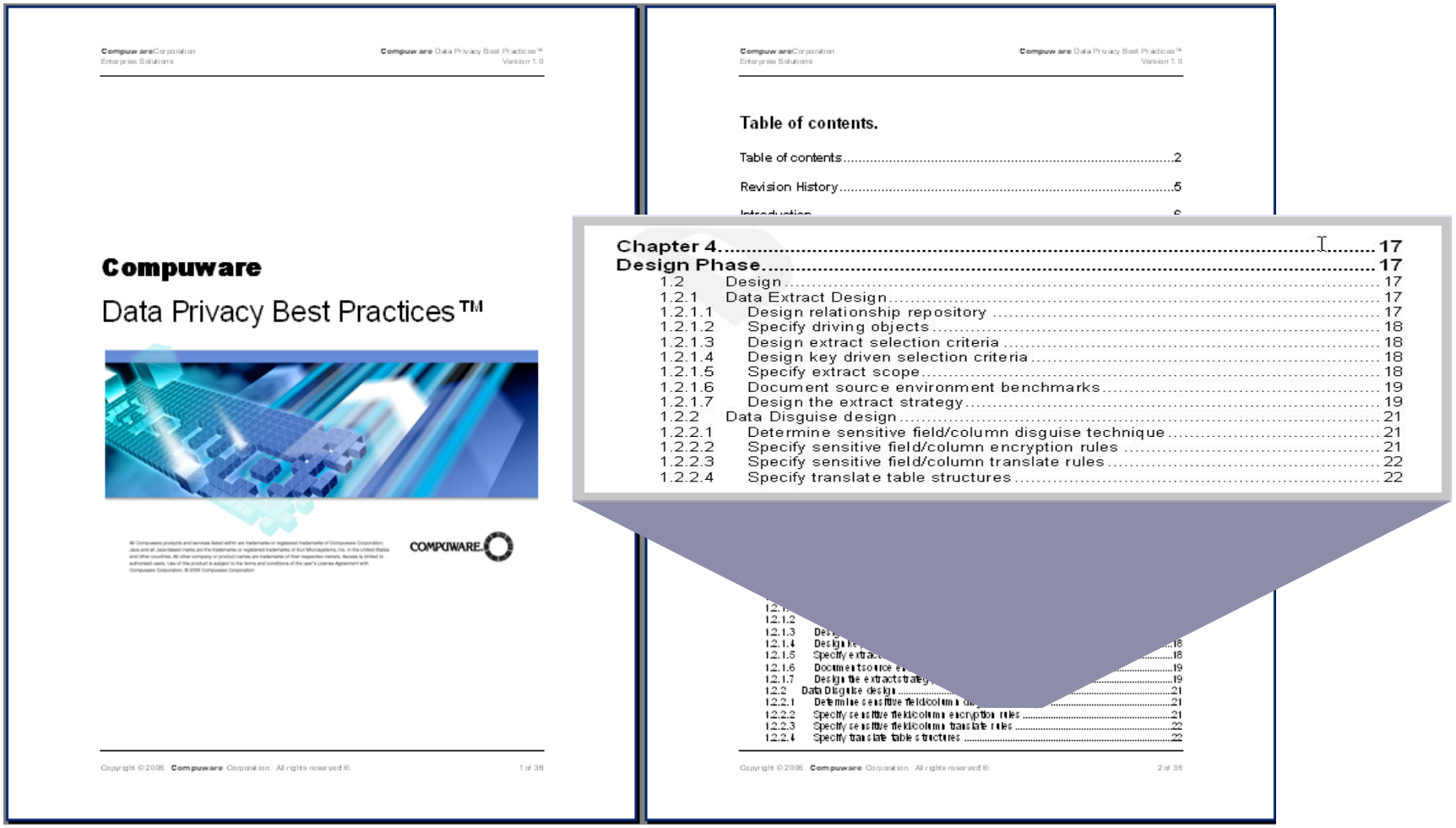
Test Data Privacy

Process: Methodology



Test Data Privacy

Process: Best Practices



Compuware

Data Privacy Best Practices™

Table of contents.

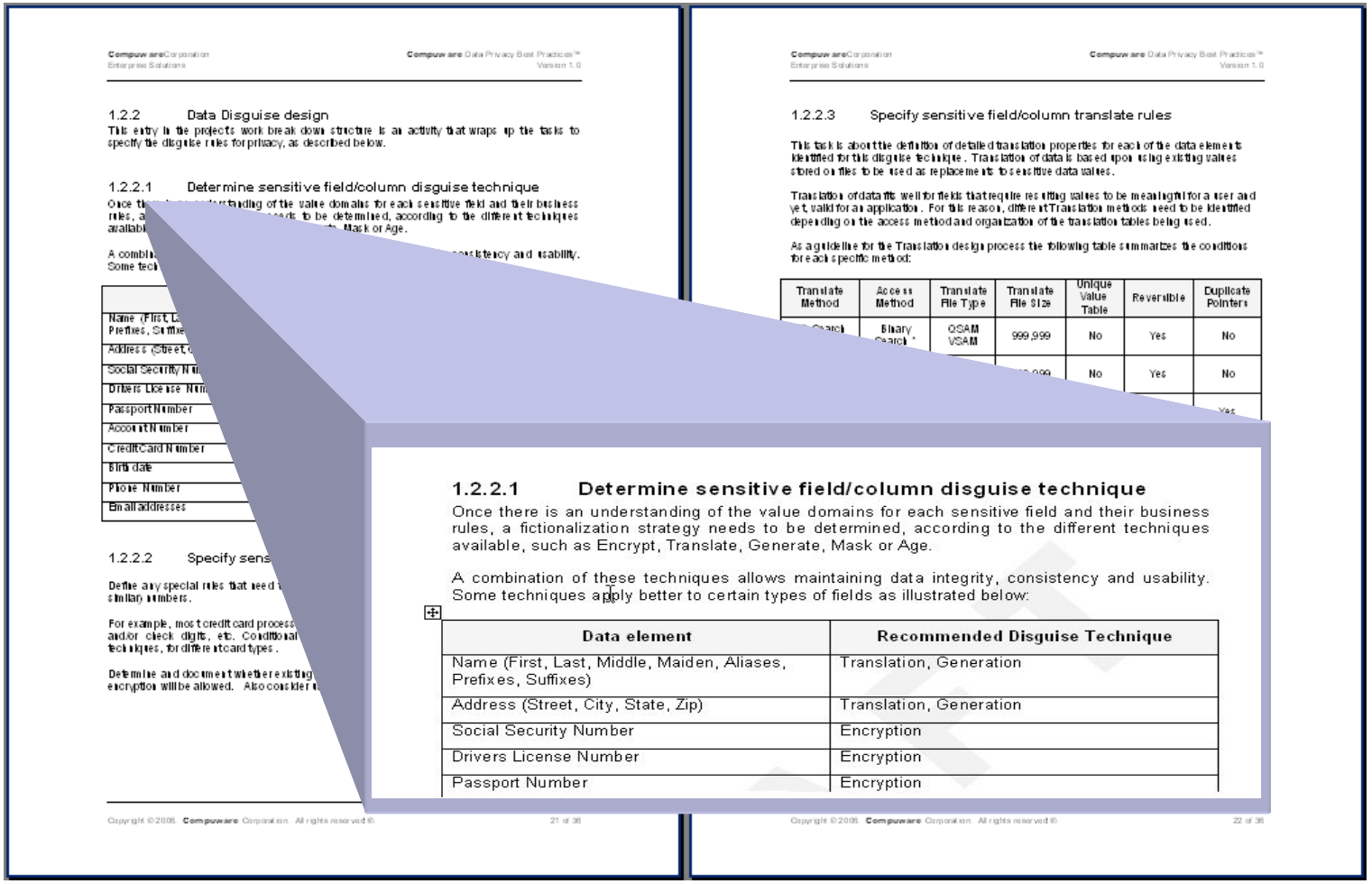
Table of contents 2

Revision History 5

Chapter 4 17
Design Phase 17
1.2 Design 17
1.2.1 Data Extract Design 17
1.2.1.1 Design relationship repository 17
1.2.1.2 Specify driving objects 18
1.2.1.3 Design extract selection criteria 18
1.2.1.4 Design key driven selection criteria 18
1.2.1.5 Specify extract scope 18
1.2.1.6 Document source environment benchmarks 19
1.2.1.7 Design the extract strategy 19
1.2.2 Data Disguise design 21
1.2.2.1 Determine sensitive field/column disguise technique 21
1.2.2.2 Specify sensitive field/column encryption rules 21
1.2.2.3 Specify sensitive field/column translate rules 22
1.2.2.4 Specify translate table structures 22

Test Data Privacy

Process: Best Practices



1.2.2.1 Determine sensitive field/column disguise technique

Once there is an understanding of the value domains for each sensitive field and their business rules, a fictionalization strategy needs to be determined, according to the different techniques available, such as Encrypt, Translate, Generate, Mask or Age.

A combination of these techniques allows maintaining data integrity, consistency and usability. Some techniques apply better to certain types of fields as illustrated below:

Data element	Recommended Disguise Technique
Name (First, Last, Middle, Maiden, Aliases, Prefixes, Suffixes)	Translation, Generation
Address (Street, City, State, Zip)	Translation, Generation
Social Security Number	Encryption
Drivers License Number	Encryption
Passport Number	Encryption

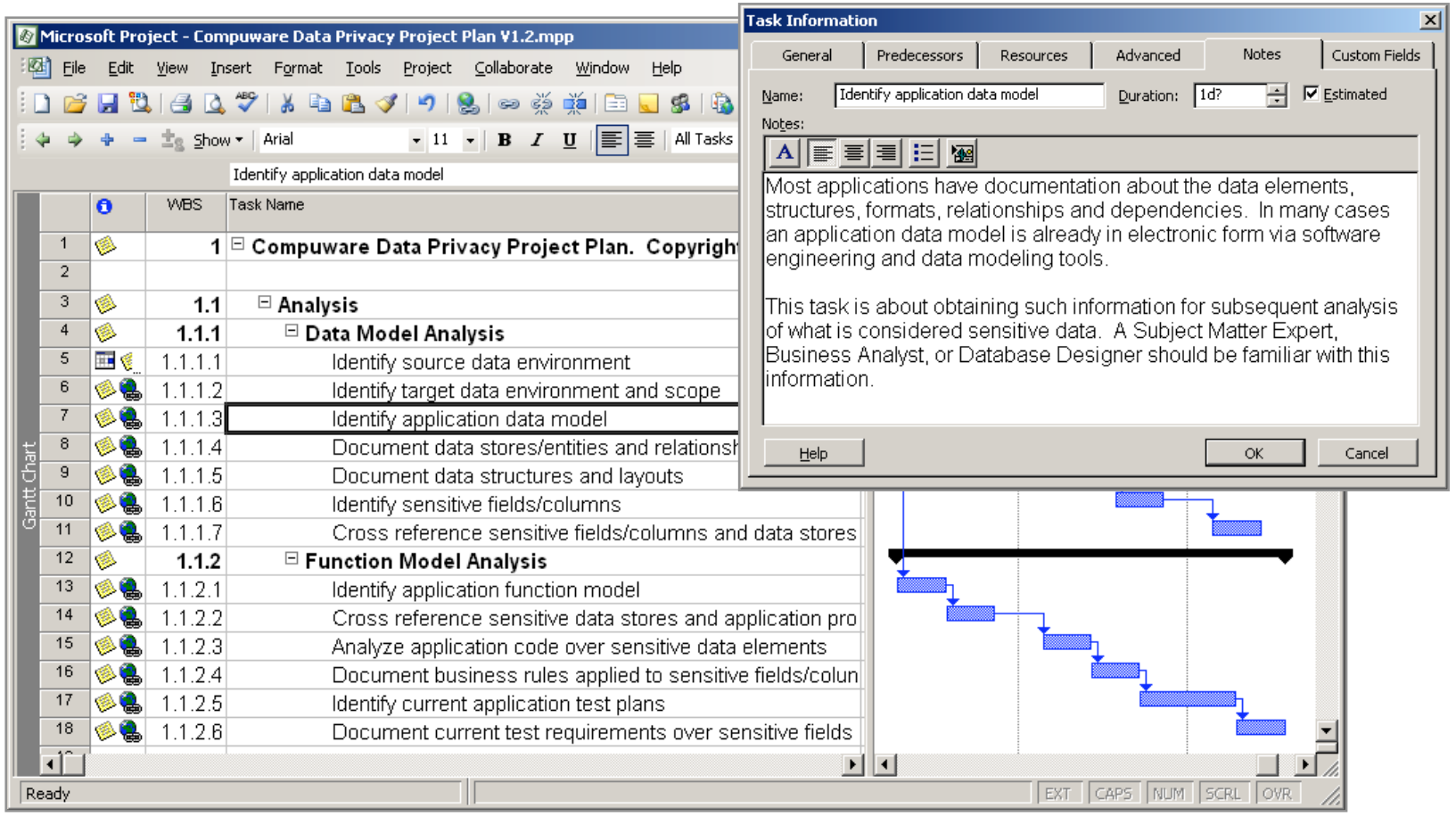
Test Data Privacy

Analyze

- **Gather and document information about:**
  - Applications to be treated
  - Data structures involved
  - Existing data relationships
  - Data Classification Scheme to understand sensitive data elements
  - Processes acting upon or impacting sensitive data

Test Data Privacy

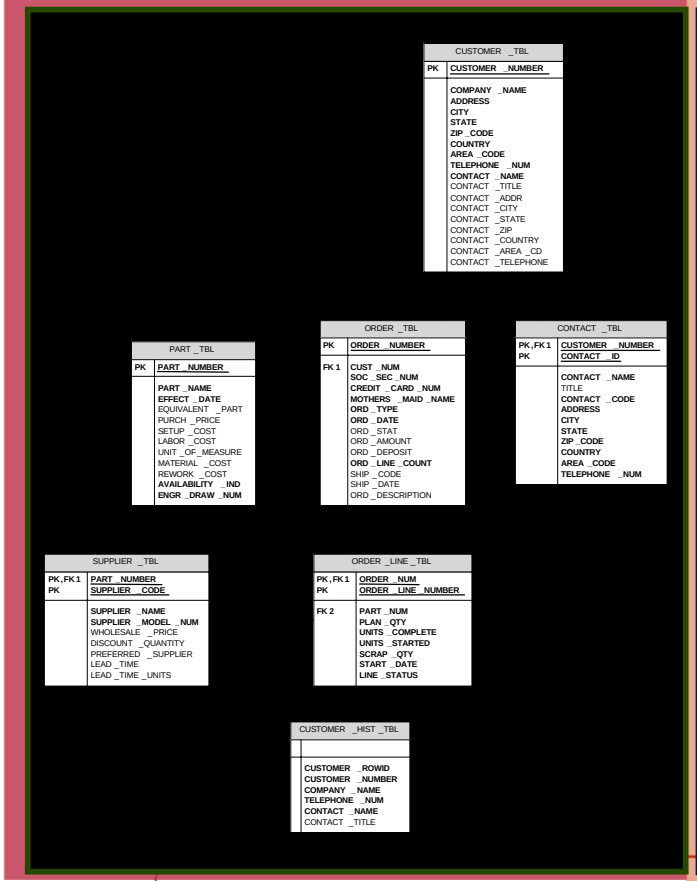
Managing the Analysis Tasks



Test Data Privacy

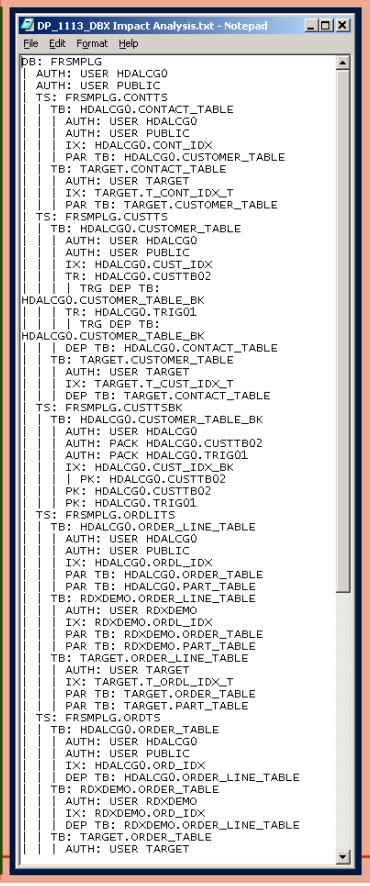
Managing the Analysis Tasks

Data Modeling Tools

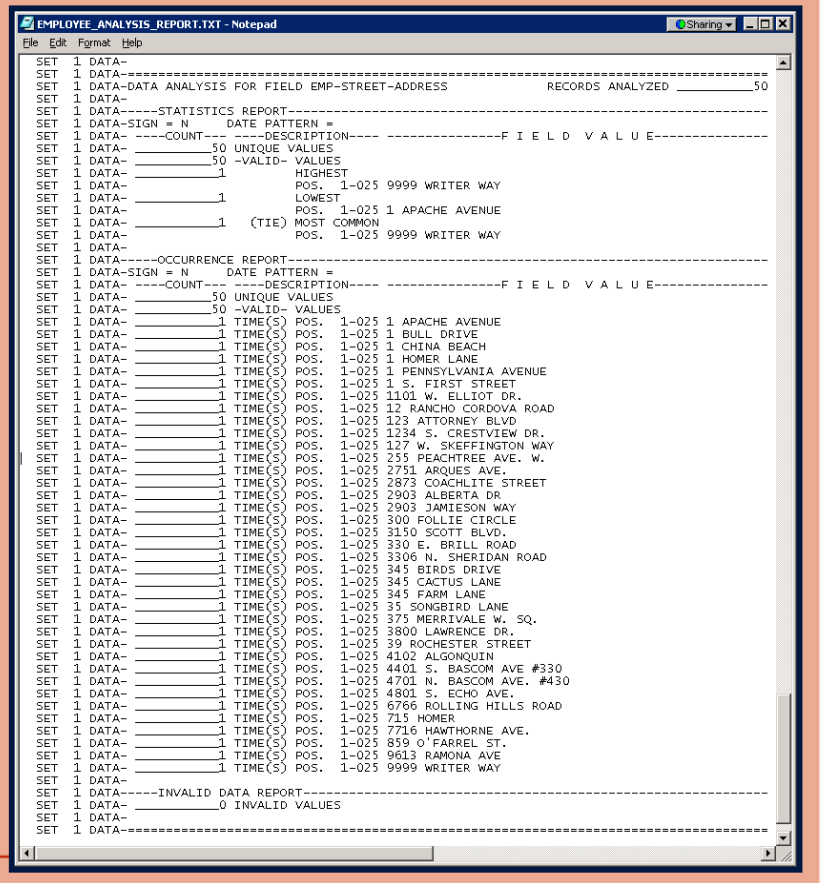


Data Management Tools

File-AID/DB2 /DBA-Xpert Impact Analysis



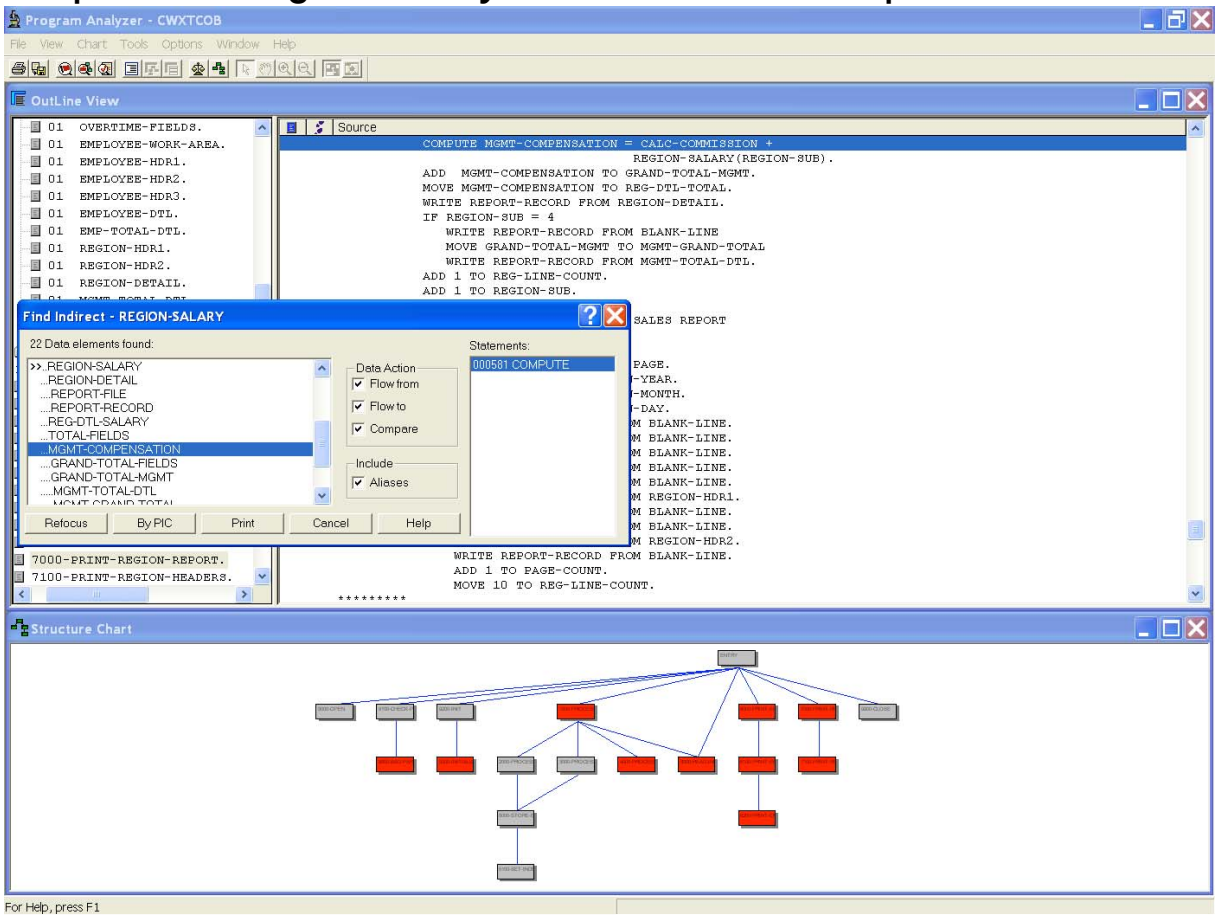
File-AID/Data Solutions Analysis



Test Data Privacy

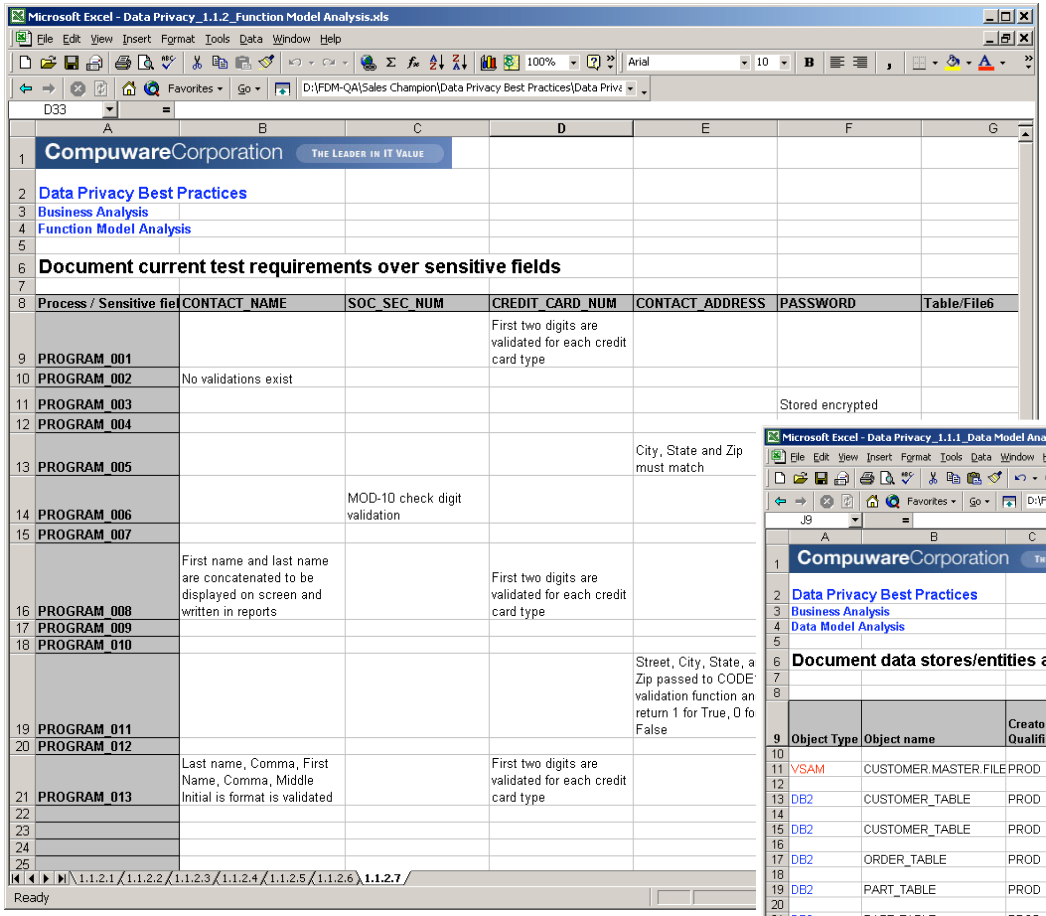
Managing the Analysis Tasks

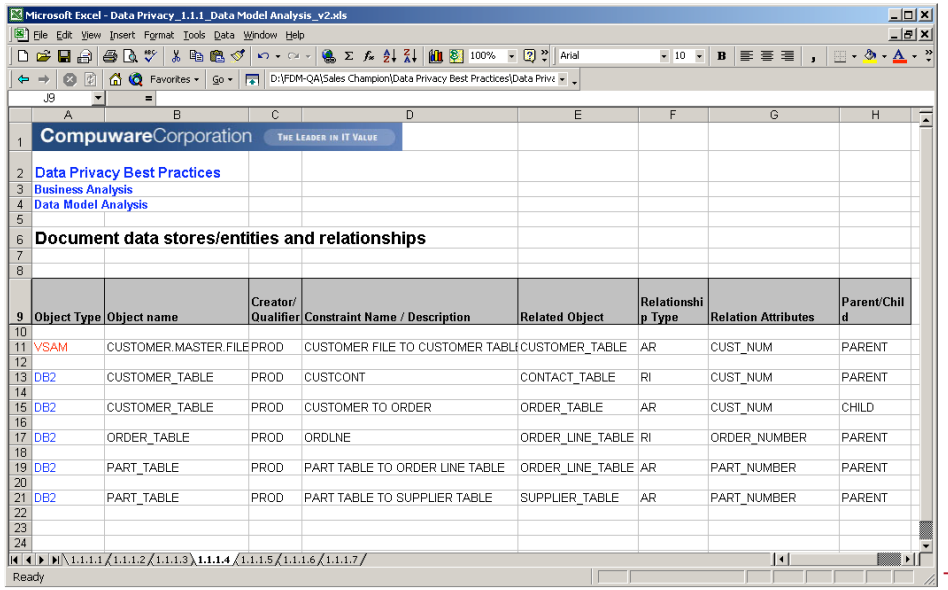
Compuware Program Analyzer for Abend-AID, Xpediter and Strobe



Test Data Privacy

Analysis Deliverables





Test Data Privacy
Design

- **Define application disguise strategy and process**
  - Source extract criteria for data (filters, naming conventions, etc.)
  - Security rules for supporting files
  - Structure, value domain (content), population strategy for translate table(s)
  - Target environment(s) and load method(s) to be used
  - Field-level obfuscation rules (encrypt, translate, age, generate)

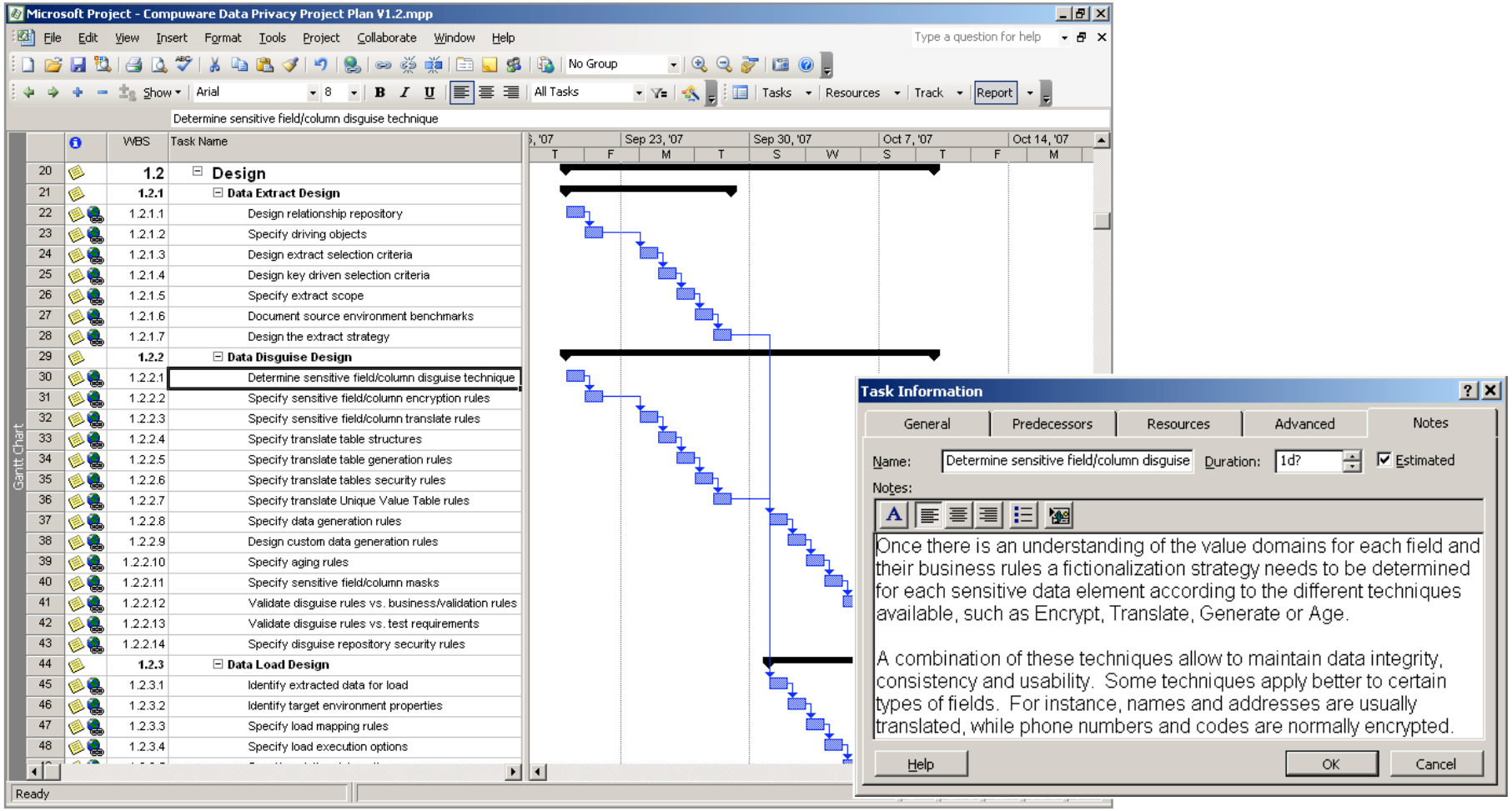
Test Data Privacy

Disguise Techniques

Encrypt	Replace sensitive values with formulated data based on a user-defined key
Translate	Replace sensitive values with meaningful, readable data using a translation table
Age	Replace sensitive dates consistently while maintaining the integrity of a date field
Mask	Conceal partial fields
Generate	Generate fictitious data from scratch or from some other source

Test Data Privacy

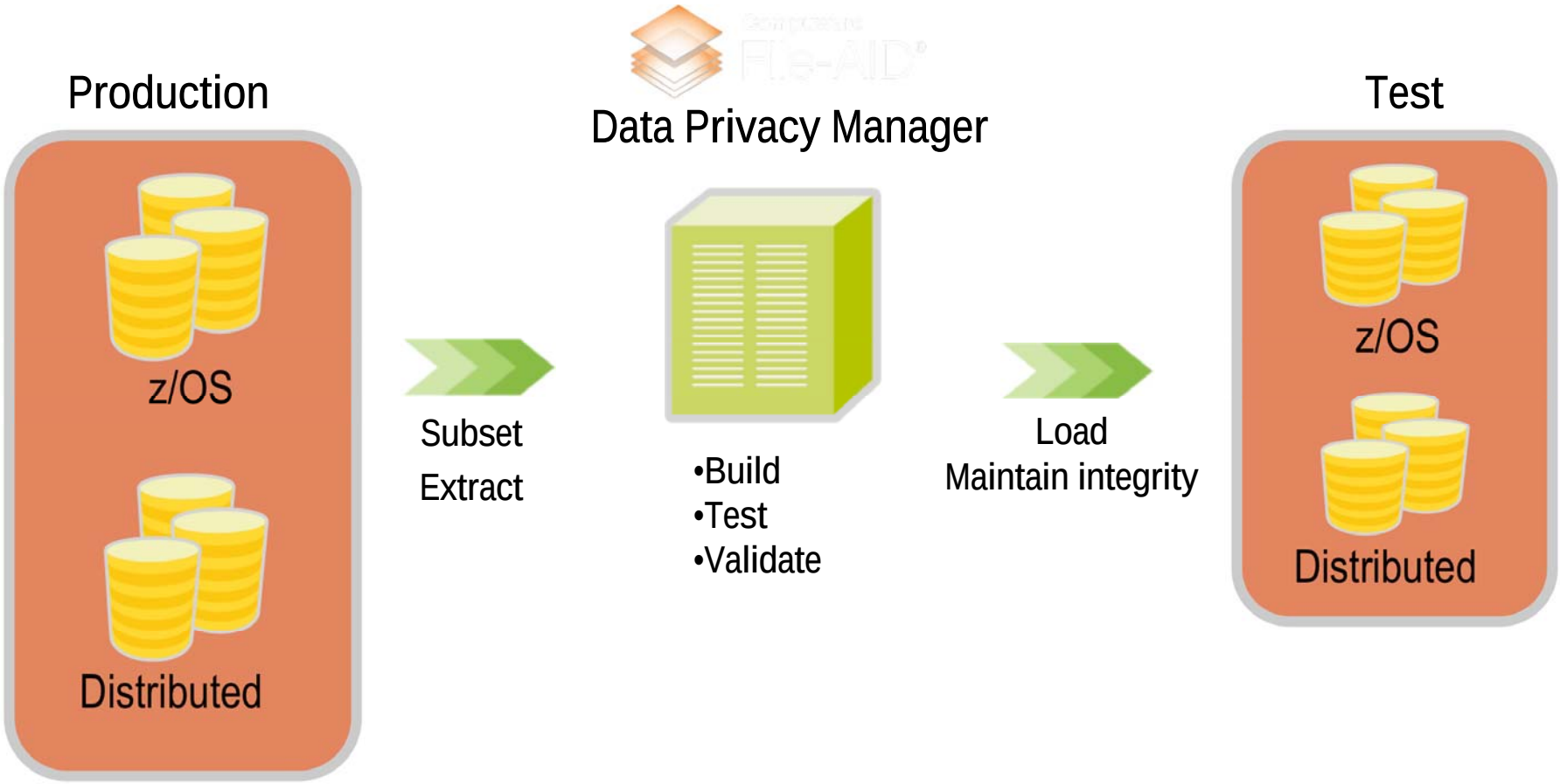
Managing the Design Tasks



	WBS	Task Name
20	1.2	Design
21	1.2.1	Data Extract Design
22	1.2.1.1	Design relationship repository
23	1.2.1.2	Specify driving objects
24	1.2.1.3	Design extract selection criteria
25	1.2.1.4	Design key driven selection criteria
26	1.2.1.5	Specify extract scope
27	1.2.1.6	Document source environment benchmarks
28	1.2.1.7	Design the extract strategy
29	1.2.2	Data Disguise Design
30	1.2.2.1	Determine sensitive field/column disguise technique
31	1.2.2.2	Specify sensitive field/column encryption rules
32	1.2.2.3	Specify sensitive field/column translate rules
33	1.2.2.4	Specify translate table structures
34	1.2.2.5	Specify translate table generation rules
35	1.2.2.6	Specify translate tables security rules
36	1.2.2.7	Specify translate Unique Value Table rules
37	1.2.2.8	Specify data generation rules
38	1.2.2.9	Design custom data generation rules
39	1.2.2.10	Specify aging rules
40	1.2.2.11	Specify sensitive field/column masks
41	1.2.2.12	Validate disguise rules vs. business/validation rules
42	1.2.2.13	Validate disguise rules vs. test requirements
43	1.2.2.14	Specify disguise repository security rules
44	1.2.3	Data Load Design
45	1.2.3.1	Identify extracted data for load
46	1.2.3.2	Identify target environment properties
47	1.2.3.3	Specify load mapping rules
48	1.2.3.4	Specify load execution options

Test Data Privacy

Develop



Test Data Privacy

Development tasks – z/OS Relationships

Production

AR/RI

```
File-AID/RDX ------------   Relationship Detail  ------------- Row 1 to 5 of 5
Command ===>                                                  SCROLL ===> CSR

Base object:    D701CW01.PROD.CUSTOMER_TBL

Line Commands:  S = Select Relationship to Modify  D = Delete Relationship
                A = Add Application Relationship   I = Relationship Information

                                                        Obj  Rel
CMD     Parent/Dependent                                Type Type      Status
--- ------------------------------------------------ ---- ----- ----------------
 _  D701CW01.PROD.CUSTOMER_TBL                       DB2  RI
      D701CW01.PROD.CONTACT_TBL                       DB2
 _  D701CW01.PROD.CUSTOMER_TBL                       DB2  AR
      D701CW01.PROD.ORDER_TBL                         DB2
 _  'SUSJDL0.FLEX.KEYFILE.EXTRACT'                   MVS  AR
      D701CW01.PROD.CUSTOMER_TBL                      DB2
 _  D701CW01.PROD.ORDER_TBL                          DB2  RI    ASSOCIATED REL.
      D701CW01.PROD.ORDER_LINE_TBL                    DB2
 _  D701CW01.PROD.PART_TBL                           DB2  RI    ASSOCIATED REL.
      D701CW01.PROD.ORDER_LINE_TBL                    DB2
****************************** Bottom of data ********************************
```

Test Data Privacy

Development tasks – z/OS Extract Scope

Production

AR/RI

```
File-AID/RDX ----- Graphical Relationship Display ---------- Row 1 to 11 of 11
Command ===>                                                 SCROLL ===> PAGE

TAB to Table and press ENTER for an Option List
* Denotes the table is involved in additional relationships

 DB2-PART_20
   |
   |__ DB2-ORDER_LINE_20                                                  *
   |
   |__ MVS-'EU.TRANSFER.TRAIN.FDM.PART20.UNLOAD'


 DB2-ORDER_TABLE
   |
   |__ DB2-ORDER_LINE_20                                                  *
```

Test Data Privacy

Development tasks – Disguise z/OS Extract

Production

Subset Extract

```
File-AID/RDX ------------------  Extract Menu  --------------------------------
Option ===>                                              USER Profile: ENCRYPT1
                                                                 SSID: D701

Primary commands: menu-number, ALL, REFerence, REQuest, MODE
   Line commands: S or / to create flow through selected options.

Description  ===> USING ENCRYPTION DB2-TEST.CUSTOMER_TABLE

                                 Current Values
 _  1  Driving Object            DB2-TEST.CUSTOMER_TABLE
 _  2  Extract Scope and         Dir=Y, Par=Y, Sib=Y, Ind=Y, Cycles=*
       Detailed Extract Views    5 of 5 Relationships Active
 _  3  Unrelated Objects         None
 _  4  External Key File         None
 _  5  Selection Criteria        None
 _  6  IMS Key File              There are no IMS Relationships defined
 S  7  Extract File DISGUISED    SUSJDL0.V4R2M0.ENCRYPT1.EXTRACT
 _  8  Continue with Load        NO
 _  9  Save Extract Request      SUSJDL0.V4R2M0.ENCRYPT1.REQEUST(CUSTOMER)
 _ 10  View JCL
 _ 11  Submit JCL
```

Test Data Privacy

Development tasks – Disguise Set Up

Data Privacy Manager

- Build
- Test
- Validate

```
File-AID/Data Solutions ------- Criteria Menu --- TEMPORARY -----------------
OPTION ===> _

                                                              - Status -
    0   OPTIONS              - Selection criteria options     default
    1   DATE AGING           - Aging criteria                 1   sets
    2.1 EURO CONVERSION      - Euro Conversion criteria       0   sets
    2.2 TRIANGULATION        - Currency Triangulation         0   sets
    3.1 DATE PATTERN ANALYSIS - Date Pattern criteria         0   sets
    3.2 VALIDATION           - Validate criteria              0   sets
    3.3 DATA ANALYSIS        - Data Analysis criteria         0   sets
    4   TRANSLATOR           - Data Translator criteria       1   sets
    5   GENERATOR            - Data Generator criteria        1   sets
    6   FIELD EXITS          - Utilities criteria             0   sets
    7   DATA ENCRYPTION      - Data Encryption Criteria       1   sets

Member list description ===> _____________________________

    Long    ===> _____________________________________________________________
Description ===> _____________________________________________________________

Use ENTER to continue
Use VIEW to display criteria request   SAVE to write criteria request
Use END to return to Input Spec Panel  CANCEL to restart at Input Spec Panel
```

Test Data Privacy

Development tasks – z/OS Load

```
File-AID/RDX --------------------  Load Menu  ---------------------------------
Option ===> _                                          USER Profile: RDXMENU

Primary commands: menu-number, ALL, REFerence, REQuest, MODE
   Line commands: S or / to create flow through selected options.

Extract File name ===> HFHSAS0.SCOTT.RDX.EXTRACT
Description       ===> DB2-FRSAMP.CUST_STUFF

                                 Current Values
 _  1  Load Object Specifications  SSID=D701, Load Method=SQL Insert
 _  2  Source/Target Mapping       0 of 6 Objects are excluded
 _  3  Target Environment          Create: Tables=6 + DB, Files=0
 _  4  Existing Data Options
 _  5  Insert Processing Options
 _  6  Save Load Request           None
 _  7  View JCL
 _  8  Submit JCL
```

Disguised Extract

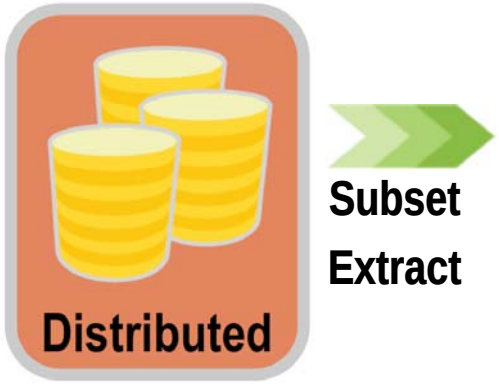
Load
Maintain
integrity

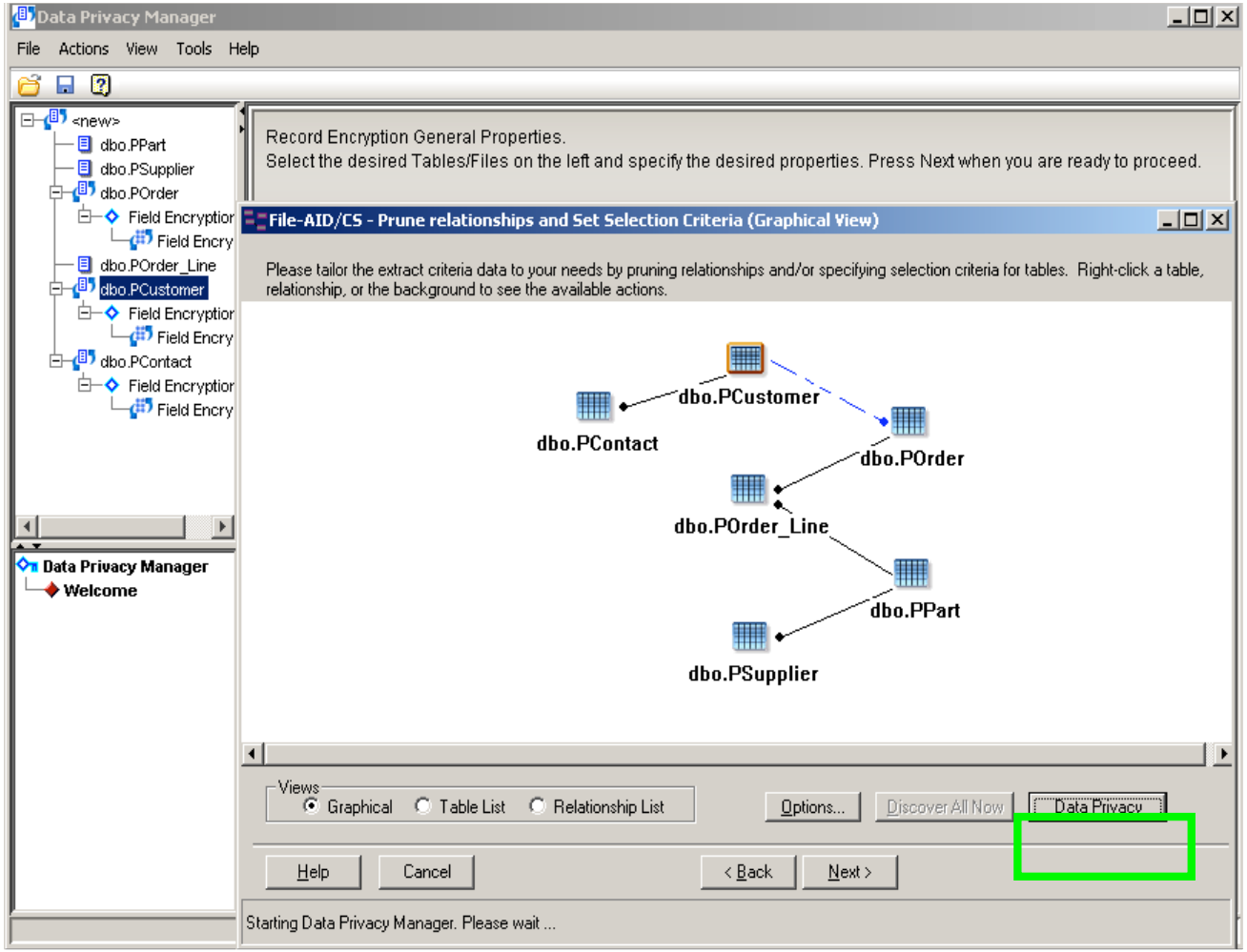
Test

Test Data Privacy

Development tasks – Distributed Extract

Production



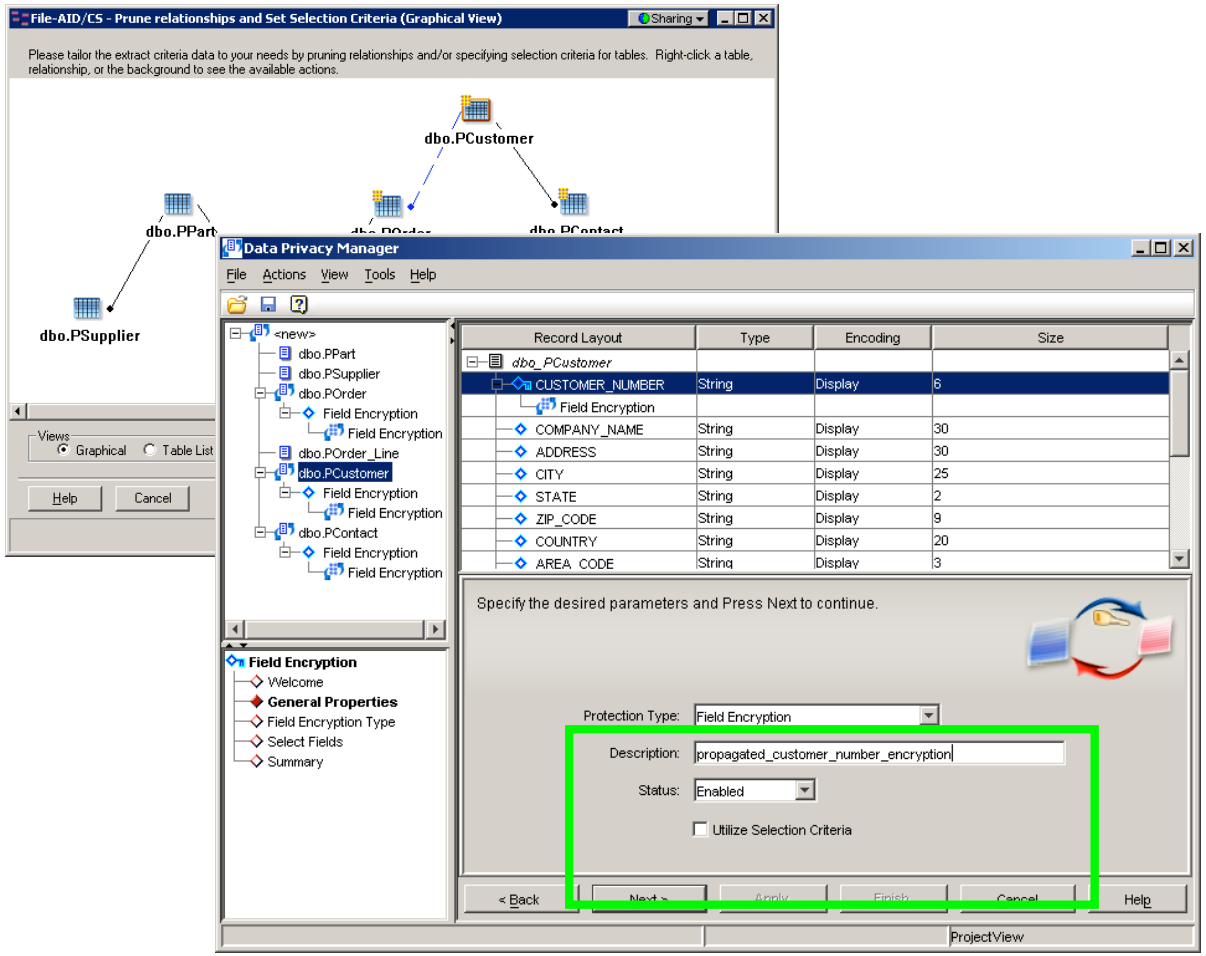


Test Data Privacy

Development tasks – Distributed Disguise

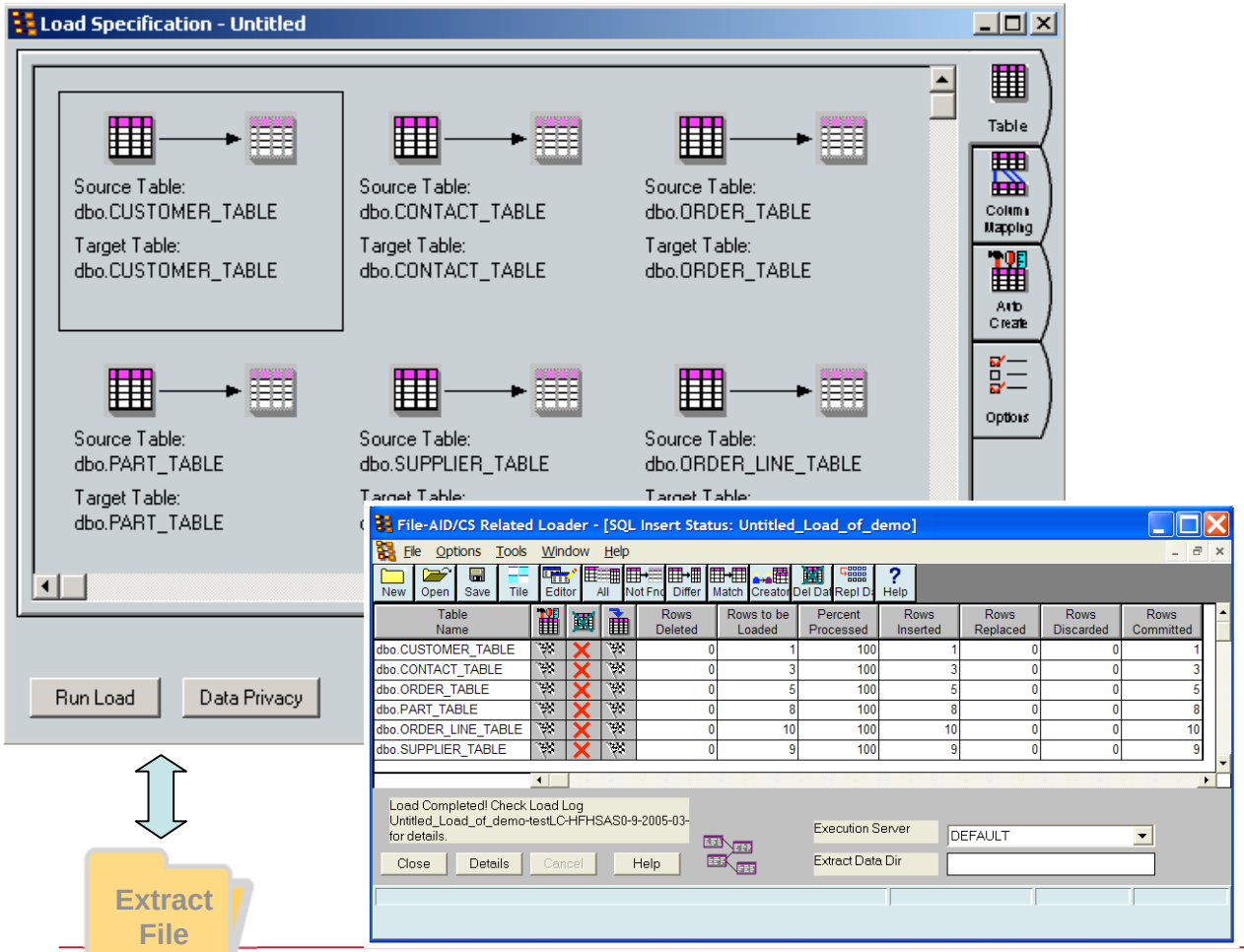
Data Privacy Manager

- Build
- Test
- Validate



Test Data Privacy

Development tasks – Distributed Disguise



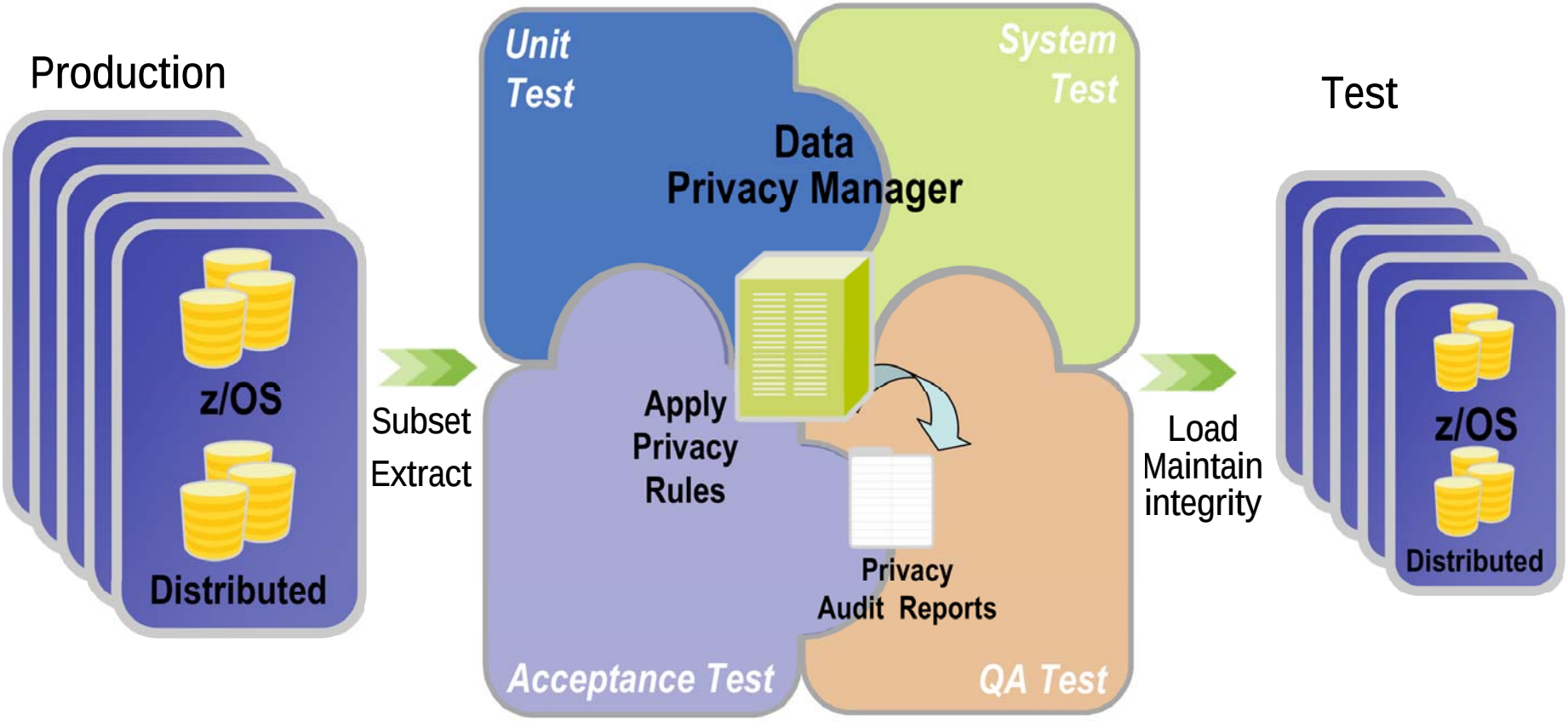
Load
Maintain
integrity

Test

Distributed

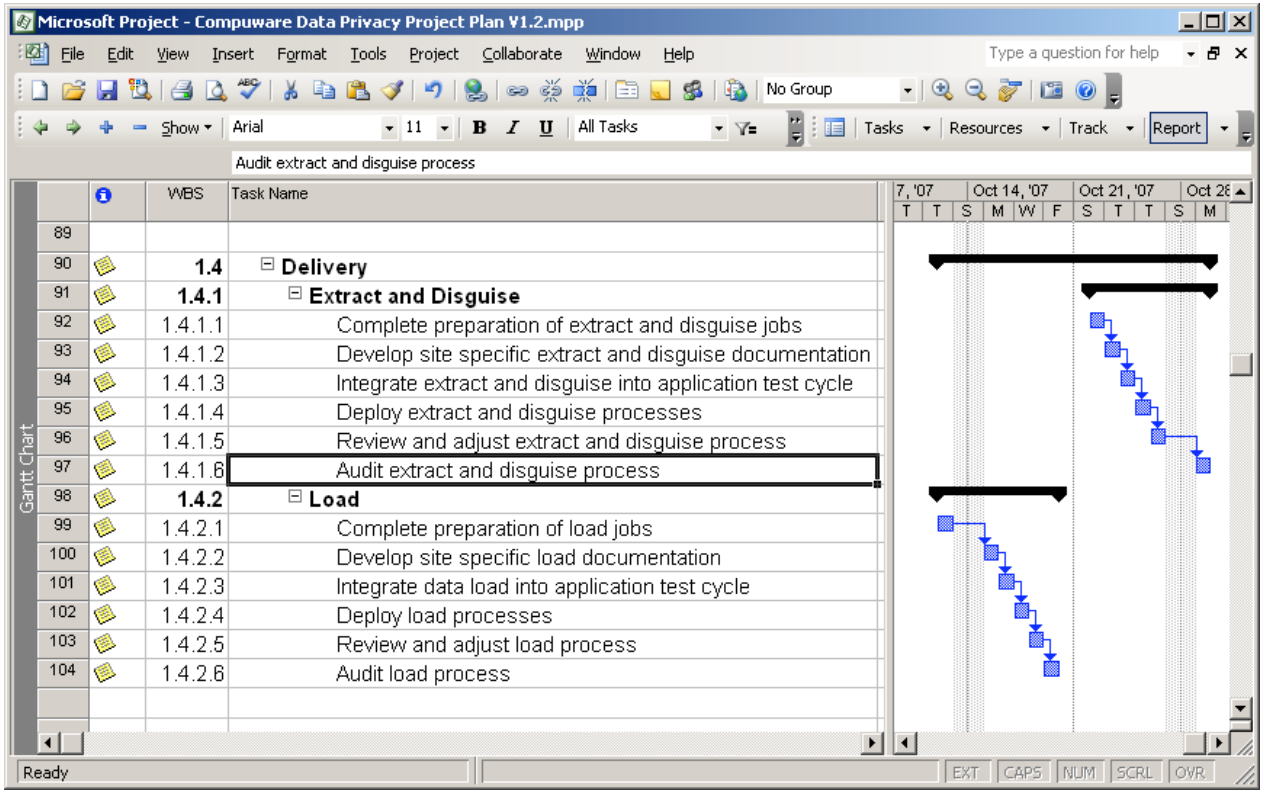
Test Data Privacy

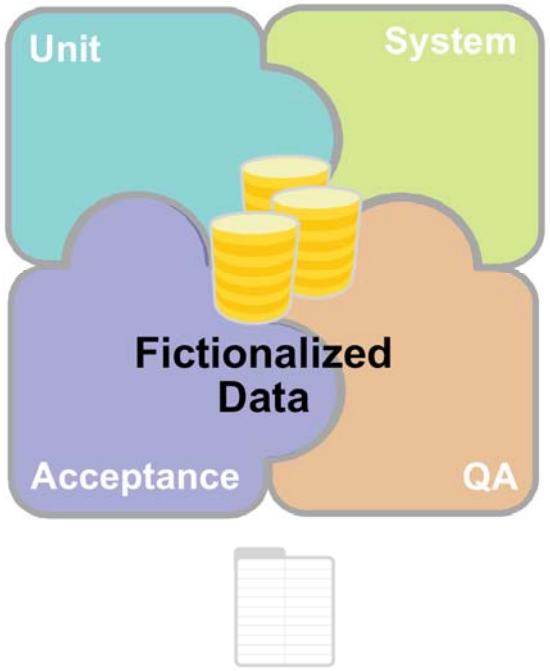
Delivery



Test Data Privacy

Managing the Delivery Tasks





Privacy Audit Reports

Test Data Privacy

Delivery – Output Results

Original Data	Disguised Data	Rule Applied
Mary Ward	Jill Jones	Translated
03-20-1962	04-18-1962	Aged
104 Main Street	111 State Avenue	Translated
Flint, MI 48025	Flint, MI 48025	Unchanged
370-55-2939	431-81-6492	Encrypted
4294 5730 5839 3037	42XX XXXX XXX9 3037	Masked
$300,000	$126,877	Encrypted
null	(810) 609-2873	Generated

Test Data Privacy

Delivery – Audit Reports

```
****** ***************************** Top of Data ******************************
000100 01 NOV 2005  13:03:36        FILE-AID/RDX 4.2    DISGUISE AUDIT TRAIL
000110 EXTRACT FILE : SUSJDL0.V4R2M0.EXTRACT.TRANS
000130 SOURCE OBJECT: D701CW01.PROD.ORDER_TBL
000140
000190                                        SUMMARY INFORMATION
000400
000500 AUDIT TRAIL FILE PRINTED:  SUSJDL0.RDXA.D008.D051021.T140525
000600 UPDATE NUMBER:        1   ACTION: CHANGE
000611 DATA DISPLAYED             ----+----1----+----2----+----3----+----4----+
000613  BEFORE      POSITION 1    AA1111 CC3300 268-80-9611 WILLIAMS         TO
000630   CHANGE--->                             ** **** ********
000650  AFTER       POSITION 1    AA1111 CC3300 268-39-2877 JONES            TO
000700 ==========================================================================
****** ***************************** Bottom of Data ***************************
```

```
RECORD NUMBER:                1 ACTION: CHANGE     RECORDED: 1 Nov 2005 AT 12:33:33

DATA DISPLAYED                ----+----1----+----2----+----3----+----4----+----5----+

Before:                       AA1111|CC3300|268-80-9611|WILLIAMS          |TOM
Fields with DP Applied:                |      ** **** |********           |
After:                        AA1111|CC9422|268-39-2877|JONES             |TOM
```

RIVACY AUDIT TRAIL

Test Data Privacy

Delivery - Disguise Rule Administration

Data Privacy Manager

Disguise Rules

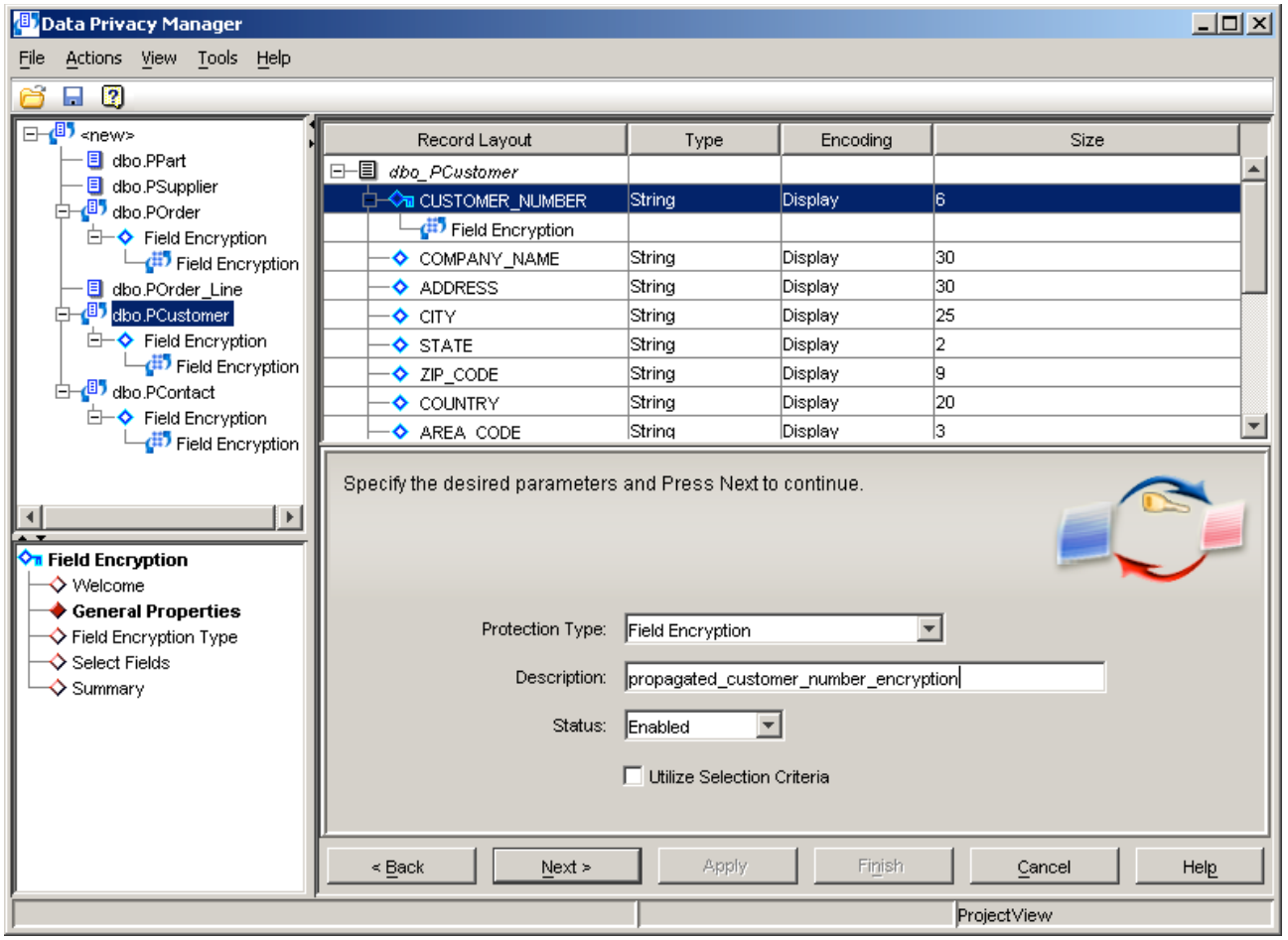
```
File-AID/RDX -----------  Data Disguise - Object List  ------- Row 1 to 5 of 5
Command ===>                                                  Scroll ===> CSR

Primary Commands: ObjectIn, ObjectOut, Find, Size
   Line Commands: S = Select     I = Info
                  O = ObjectOut  R = Related objects  L = List DB

  SSID: D701 Location: D701CW01
  Object Name                                  Disguised Columns/Fields      +
  ------------------------------------------- ------------------------------
_ PROD     CONTACT_TBL                        CONTACT_NAME, CUSTOMER_NUMBER
_ PROD     CUSTOMER_TBL                       CUSTOMER_NUMBER
_ PROD     ORDER_LINE_TBL
_ PROD     ORDER_TBL                          SOC_SEC_NUM, CREDIT_CARD_NUM, CU
_ PROD     PART_TBL
****************************** Bottom of data ********************************
```

Test Data Privacy

Delivery - Disguise Rule Administration

Data Privacy Manager

Disguise Rules



Test Data Privacy

Delivery - Validation of Results

- Verify Disguised Data is Properly Testing:
  - New or modified code
  - Critical business logic
- Online and Printed Reports
- Risk Metrics
- Change Management Signoff Requirements
- Auditing Documentation

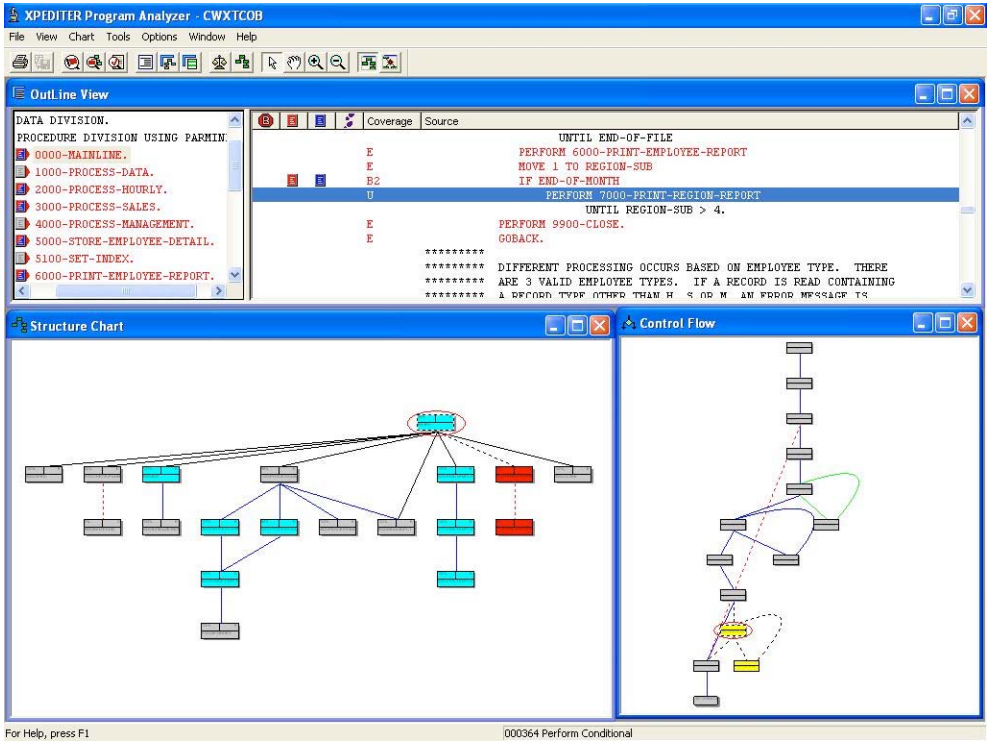
Original Data	Disguised Data	Rule Applied
Mary Ward	Jill Jones	Translated
03-20-1962	04-18-1962	Aged
104 Main Street	111 State Avenue	Translated
Flint, MI 48025	Flint, MI 48025	Unchanged
370-55-2939	431-81-6492	Encrypted
4294 5730 5839 30	42XX XXXX XXX9 3037	Masked
$300,000	$126,877	Encrypted
null	(810) 609-2873	Generated

	Risk	Verbs Executed	Total Verbs	Branches Executed
System: PDASYSTEM	1007	3961(50%)	7816	867(49%)
Load Module: PDA001	482	159(48%)	328	34(50%)
Load Module: PDA002	478	135(55%)	243	36(66%)
Load Module: PDA003	483	114(37%)	303	23(35%)
Load Module: PDA004	918	157(48%)	326	36(51%)
PDA004 (11/04/04-06:24:59) Opt=N,Debug=N	918	157(48%)	326	36(51%)
Load Module: PDA005	484	250(61%)	406	75(62%)
Load Module: PDA006	491	227(39%)	572	61(39%)
Load Module: PDA007	942	391(59%)	655	111(63%)
Load Module: PDA008	974	336(42%)	799	80(38%)
PDA008 (11/04/04-06:29:39) Opt=N,Debug=N	974	336(42%)	799	80(38%)
Load Module: PDA009	939	451(58%)	777	92(51%)
Load Module: PDA010	489	325(50%)	646	83(53%)
Load Module: PDA011	485	156(38%)	410	27(35%)
Load Module: PDA012	486	241(48%)	495	68(62%)
Load Module: PDA014	480	190(61%)	310	29(48%)
Load Module: PDA016	486	274(56%)	487	48(46%)
Load Module: PDA017	488	367(50%)	720	43(39%)
Load Module: PDA018	483	188(55%)	339	21(35%)

Test Data Privacy

Delivery – Improved Test Data

- Improve Test Coverage
  - Data flow analysis
  - Program level analysis
- Know What is Needed
- Remove Redundant Test Data for Efficiency



Test Data Privacy

Compuware experience across various industries

Financial Services Companies

- Large Australian Financial Institution
- Leading US SE Financial Services Company
- Global Financial Services Firm, Private Banking
- Midsize US Investment and Financial Firm
- US Life and Financial Services Co
- Large US / NE Investment Company
- Global Financial Services organization-Latin America

Retail

- Large Provider of PC Equipment

Manufacturing

- Financial Arm of Automotive Company

Insurance Companies

- Global European Insurance Company
- Large US / NE Life Insurance Company
- US Midwest Property & Casualty/Life/Auto Ins. Co.
- US Leading Health Insurance Company

Healthcare

- Large US Midwest Health Insurance Provider
- Leading US Integrated Healthcare Organization

Test Data Privacy: Case Study

Addressing HIPAA Compliance

- **Large Health Management Organization**
  - Public scrutiny and huge corporate liability due to data breach
  - Many of their applications were offshore
  - Complex environment containing a variety of data types

- **Solution: Compuware's Data Privacy Solution**
  - Promoted internal communication and provided strategic implementation consulting
  - Used multi phased project templates and Compuware Experts to conduct pilot

The end result: Successfully secured the test data for their initial 40 applications and continue to secure all 1500

Test Data Privacy: Case Study

Reducing Risk of Exposure

- **Largest US Consumer and Small Business Bank**
  - Needed to transmit sensitive data to different locations around the company, as well as to an offshore partner
  - Complex, heterogeneous environment with many technologies and applications
  - Required a test bed with consistent data from all applications

- **Solution: Compuware's Data Privacy Solution**
  - Used a data model to simplify managing disguise data consistency across enterprise systems
  - Implemented top 8 high risk applications

The end result: Successfully de-identified data for high risk applications, maintaining usability and integrity for internal and offshore use

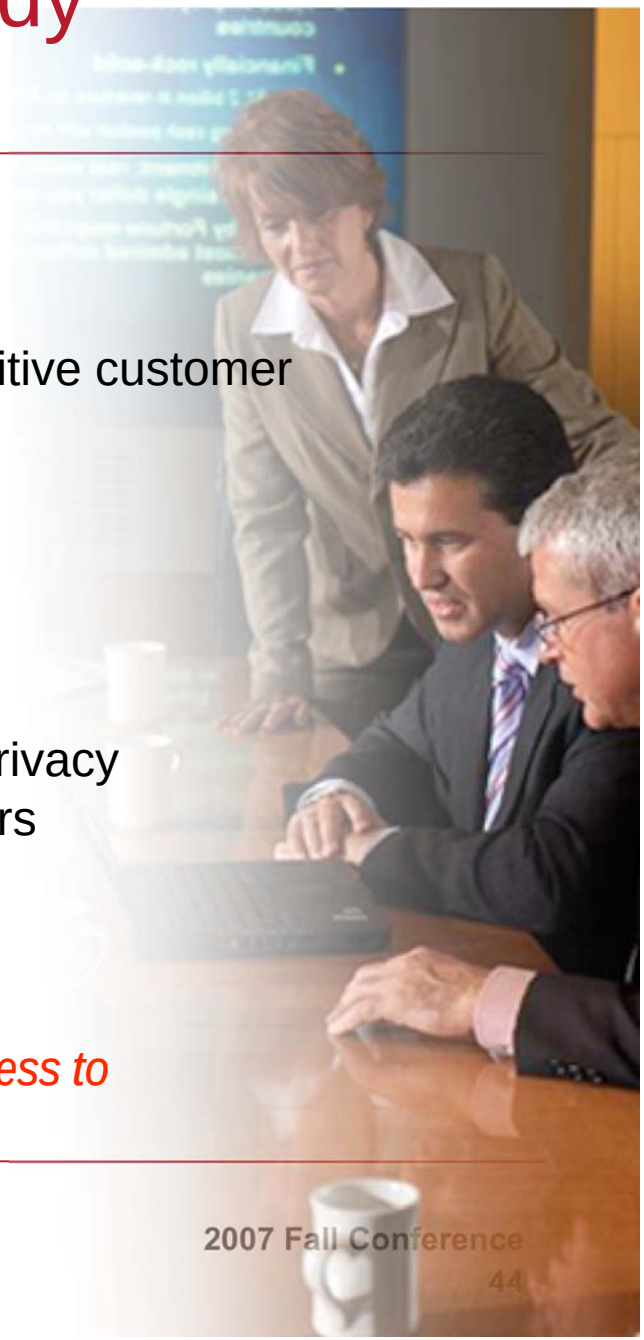
Test Data Privacy: Case Study
SOX/GLB Compliance

- **Property & Casualty / Life / Auto Insurance Co.**
  - Executive Management saw internal risk
  - Wanted to disguise SSN, DL# and Last Name in Test & Dev.
  - Required disguising z/OS DB2, AS400/DB2 data

- **Solution: Compuware's Data Privacy Solution**
  - Defined disguise rules to sensitive field elements
  - Created extract disguise jobs to disguise sensitive data
  - Provide audit reports as needed to substantiate compliance

The end result: Successfully automated a repeatable process for protecting sensitive data

Test Data Privacy: Case Study
SOX/GLB/SEC Compliance



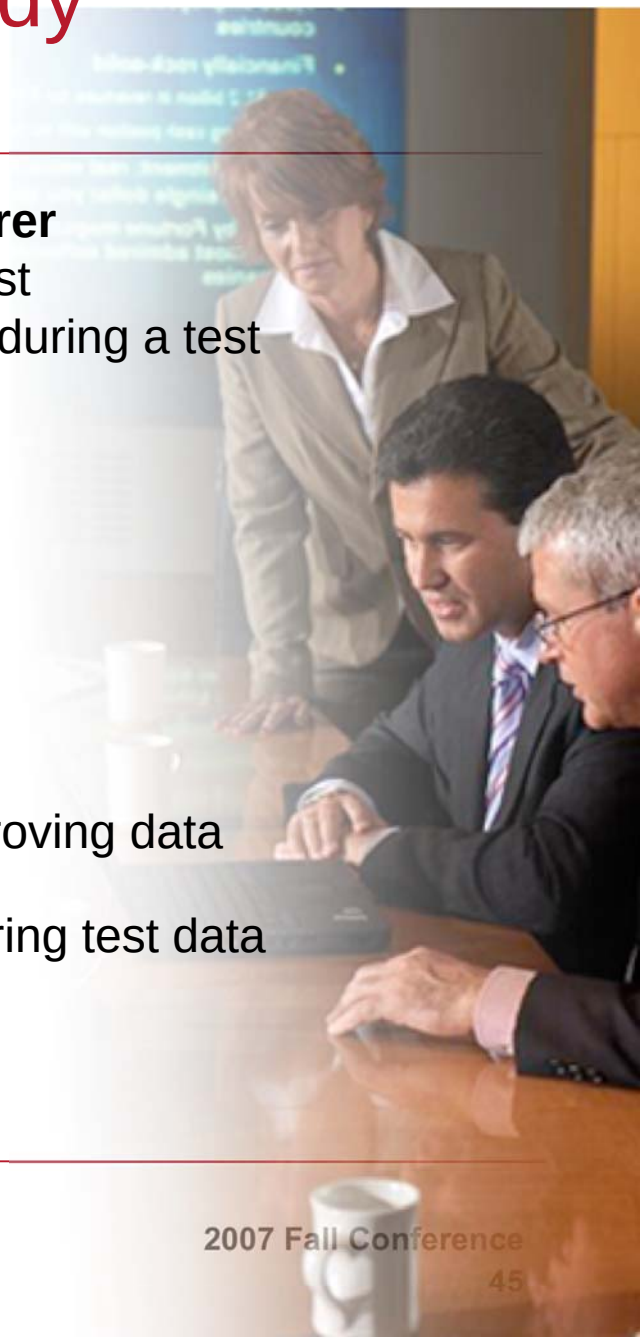
- **Financial Services Firm**
  - Highly sensitive financial data
  - Millions of financial transactions containing sensitive customer data
  - Required disguising data enterprise wide
  - IT Risk and Security is top priority

- **Solution: Compuware's Data Privacy Solution**
  - Lower cost of regulatory compliance
  - Reduced risk and liability associated with data privacy
  - Deter misuse and exposure to unauthorized users

The end result: Provided an auditable disguise process to substantiate compliance

Test Data Privacy: Case Study

Reducing Risk of Exposure



- **Leading Direct Consumer Electronics Manufacturer**
  - Discovered liability of using production data in test
  - Accidentally sent out bogus invoices and emails during a test cycle
  - Responding to enterprise-wide business process improvement initiatives such as:
    - Test driven development
    - Automated quality assurance
    - Global data management

- **Solution: File-AID/CS**
  - Increased the frequency of test cycles while improving data quality
  - Prevents database and application downtime during test data preparation

The end result: Sanitize PII to protect from privacy abuse and meet audit requirements

Test Data Privacy: Case Study

Reducing Risk of Exposure

- **$2B Securities Company**
  - Dedicated to safe/secure test data for investment products
  - Passes client files to outside vendors and 0ff-shore exposure to critical data
  - Heavy IAM and Sybase usage requiring cross-platform consistency
  - Stringent Sr. Management security expectations

- **Solution: Compuware's Data Privacy Solution**
  - Analyzed critical fields for consistency/symmetry
  - Utilization of multiple disguise techniques
  - Provides test data cleansing, consistency and congruency across platforms, audit trails, and the ability to handle volume processing

The end result: Delivered Phase-1 of the disguise project within their timeframes, on-budget

Test Data Privacy: Case Study

SOX/GLB/Insurance Compliance

- **Large Mutual Life Insurance Company**
  - Executive Management saw internal risk of exposing sensitive production data
  - Were impacted by various state insurance laws
  - Requirement to disguise the Consumer System application first which included z/OS and Oracle data
- **Solution: Compuware Test Data Privacy Solution**
  - Data Disguise routines needed to be reversible during early phases of implementation so downstream systems would not be impacted
  - Defined disguise rules for consistent results on z/OS and Oracle data
  - Translate tables were populated from data in the distributed environment and moved to the mainframe for consistent disguise

The end result: Created a repeatable process to subset and disguise data which included audit reports for validation

Test Data Privacy

Why Compuware? Our Solution is Comprehensive!

We deliver a comprehensive solution that includes:

- Integrated and proven technology
  - File-AID/Data Solutions, File-AID/RDX, and File-AID/CS
- Defined, repeatable processes for automated product execution
- Project templates that fully document the tasks for each step in the process
- Documentation to substantiate compliance
- Product-generated, standardized reports for ongoing auditability
- People with project management and data privacy implementation experience

Test Data Privacy

Why Compuware? We are Experienced!

- **We have assisted with implementation of nearly 40 Data Privacy Projects in the US and Canada over the past 3 years**
  - Several Test Data Privacy customers also in Europe, Australia, Latin American, Brazil and South Africa
  - Companies are mostly Insurance, Financial Services, Retail and Health Care organizations
- **We can assist with any stage of the project; analysis, design, development or delivery**
- **We have the ability to adapt to out of the box scenarios and situations**

Test Data Privacy

The Value Proposition

- Lowers cost of regulatory compliance
- Reduces risk and liability associated with data privacy
- Improves test data quality while maximizing testing efficiency
- Provides an end-to-end solution from a single company

Application Auditing

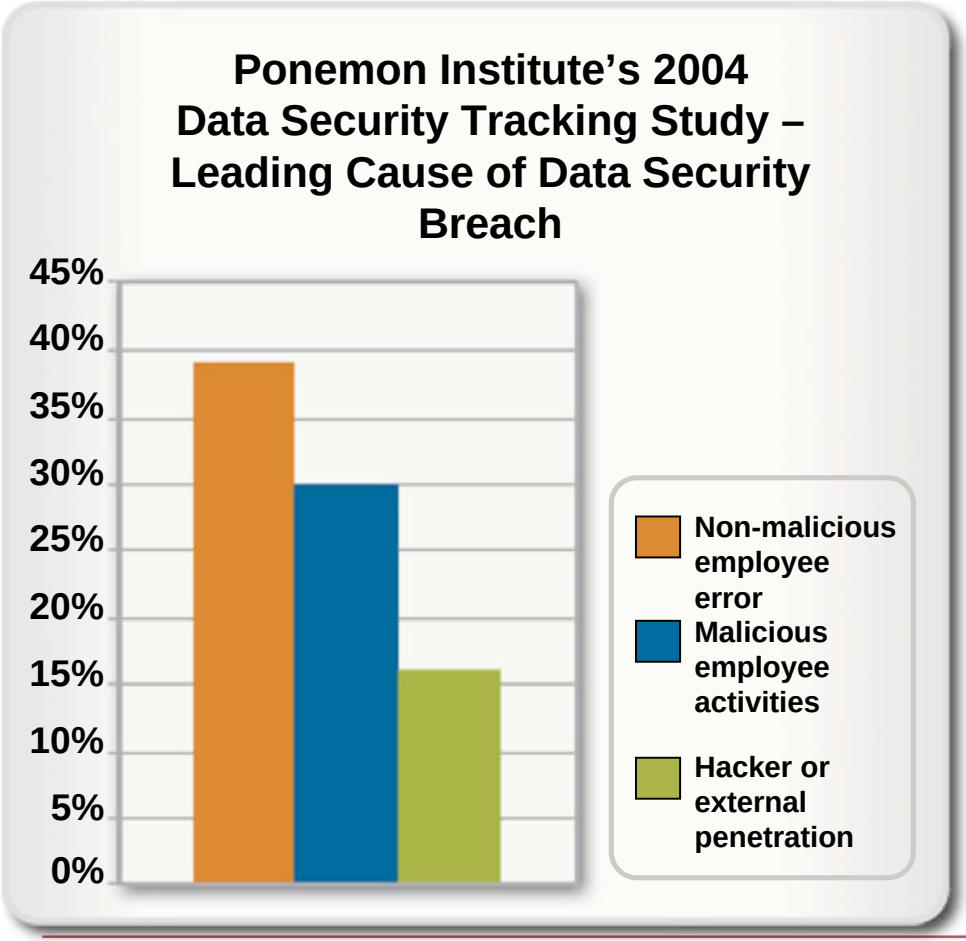
Where's Your Risk?

How do you protect against sensitive data breaches where users are authorized to access the data?

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Application Auditing

Where's Your Risk?



"Contrary to what most people believe, the majority of identity thefts are inside jobs."

Judith Collins
Michigan State University
Identity Theft Survey

"Gartner estimates that more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses."

Richard Mogull
Gartner Senior Analyst

Application Auditing
Defined

Compuware's solution for Application Auditing acts like a surveillance camera for your applications by efficiently recording internal activity between users and their applications. Not only does this deter inappropriate activities, but it also provides an audit trail that can be retrieved to investigate details of a data breach—and limit its impact.

Application Auditing

Methods currently used to prevent unauthorized access

Application

RACF, ACF2 or Top Secret **authenticate the user at login**.

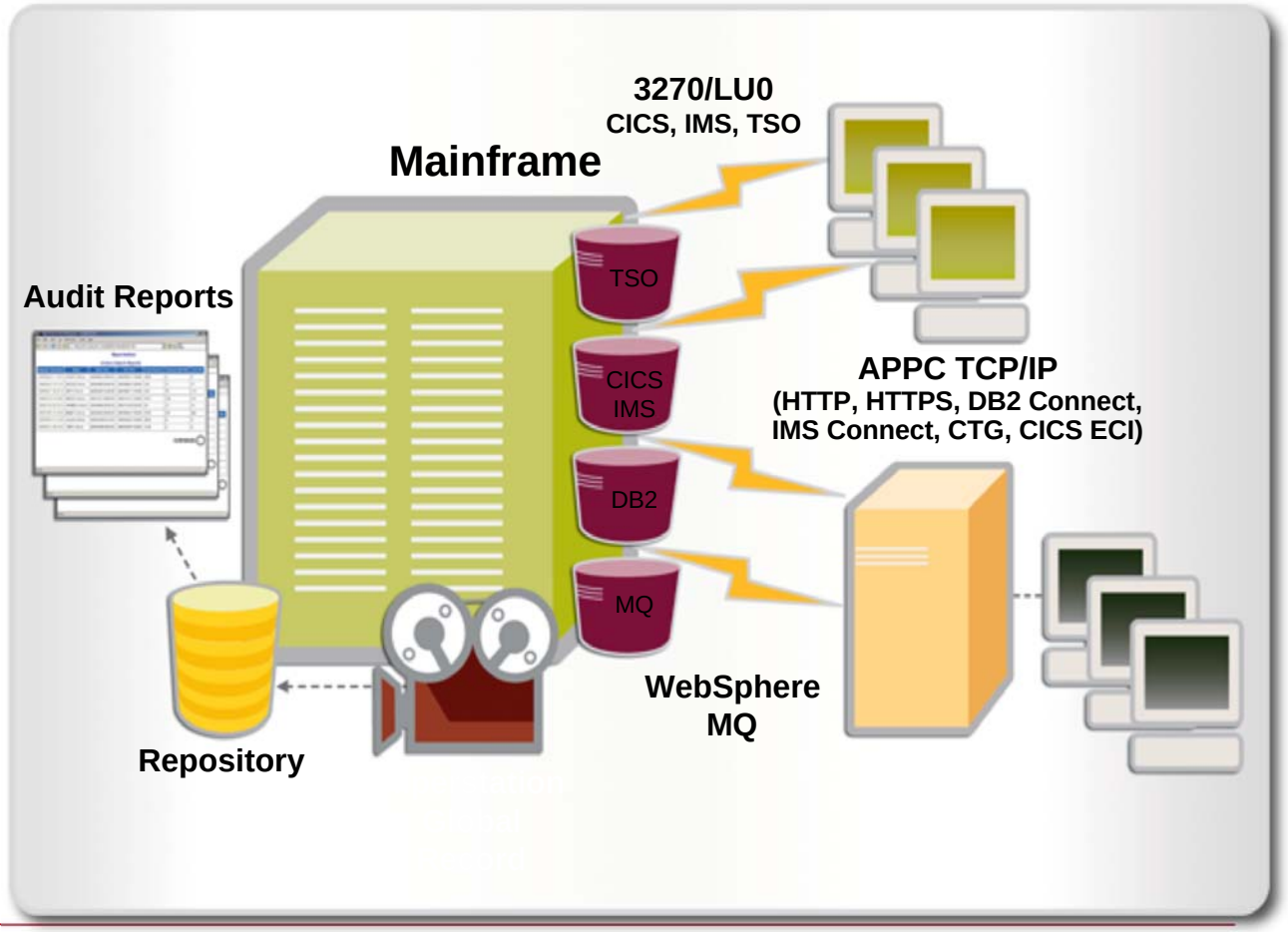
If this is done properly, you will lock out external users, but trusted internal users still have access to the application and a breach could still occur.

RACF, ACF2 or Top Secret **secure access to the application and data**.

Application Auditing

What we do: Record End-User Activity

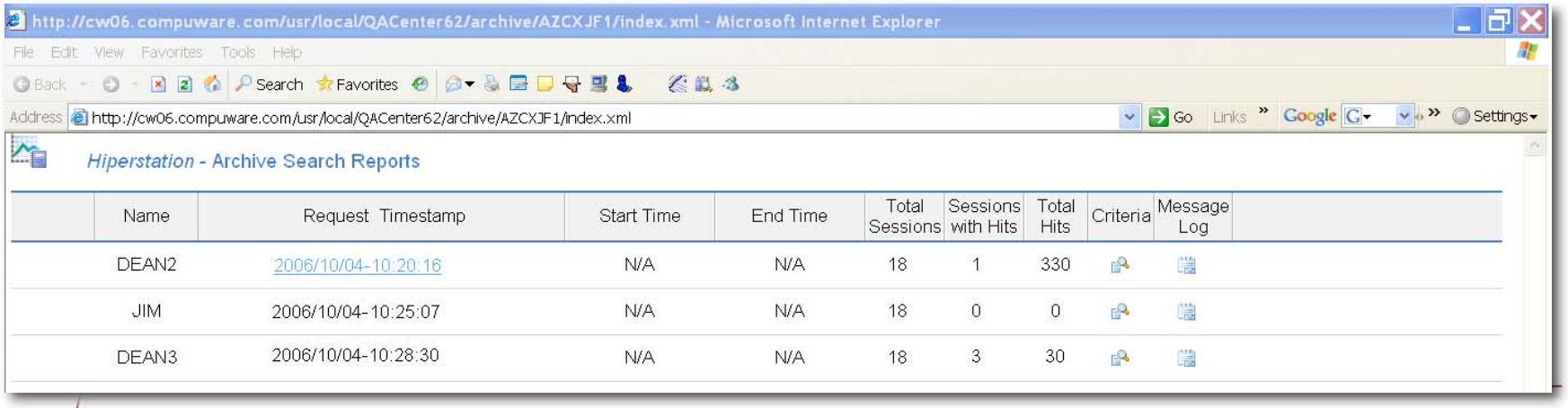
- End-users are notified that all their application activity is being recorded
- Key application communication is recorded
- Repository of Audit Trail information is saved, protected and ready for use



Application Auditing

Example of Investigating Suspicious Activity

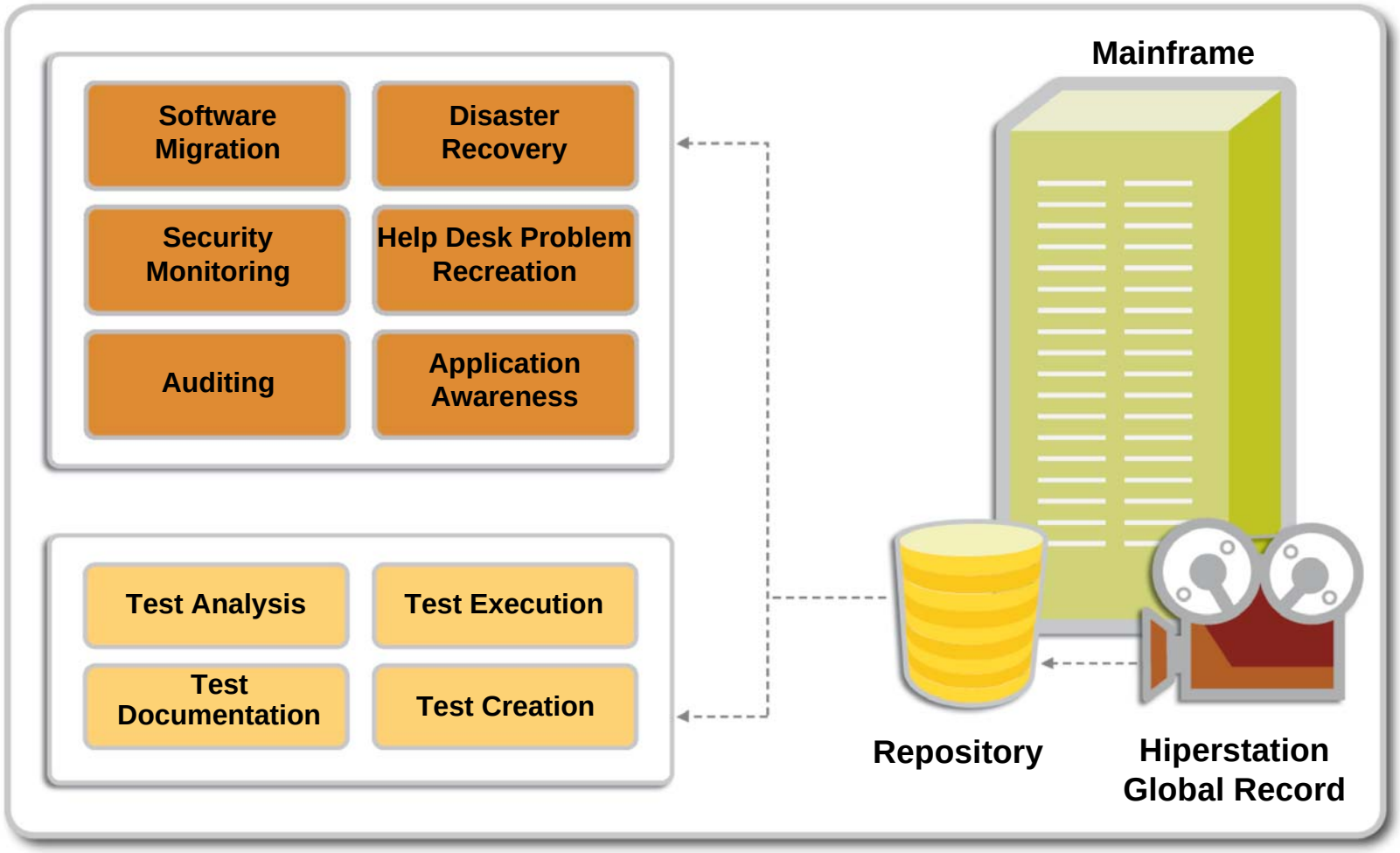
- An end-user is suspected of misusing client data
- Reports are created to pull up that user's activity from the repository
- Results are shown in a web browser
- Can focus within a date range or other criteria



Name	Request Timestamp	Start Time	End Time	Total Sessions	Sessions with Hits	Total Hits	Criteria	Message Log
DEAN2	2006/10/04-10:20:16	N/A	N/A	18	1	330		
JIM	2006/10/04-10:25:07	N/A	N/A	18	0	0		
DEAN3	2006/10/04-10:28:30	N/A	N/A	18	3	30		

Application Auditing

The Global Record Repository: *Valuable, Reusable Assets*



Application Auditing

An IT Auditor's Perspective

"As an IT Auditor, I see Compuware Hiperstation for Application Auditing as a 'proactive defense' tool. By recording end-user application activity, a company can prevent and investigate fraud and data security breaches - helping to reduce the potential for significant damage. Hiperstation's detailed forensic information and audit reports are indispensable tools that provide indisputable proof that can be used to detect problems or policy violations; prevent incidents from becoming larger; and reduce the scope of an incident response."

Paul L. Haley
IT Auditor, CISA

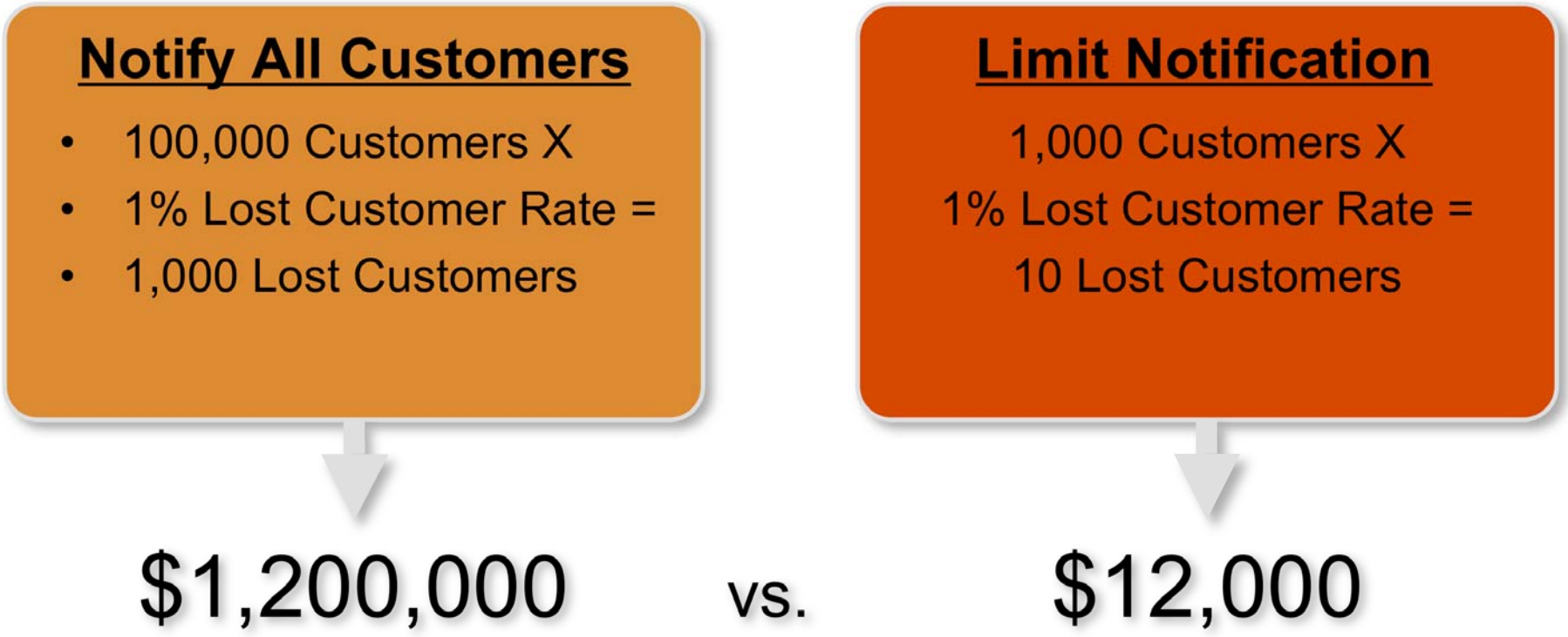
Application Auditing

Case Study Example: *An Audit Trail of Evidence*

- **Large Federal Government Agency**
  - Highly sensitive online transactions
  - Hundreds of end users all over the world producing 8+ million daily transactions
  - IT security is top priority
- **Solution: Hiperstation**
  - Record and save all application traffic
  - Search repository for suspected misuse
  - Use information for legal proceedings

Application Auditing:
Savings With a Targeted Notification

Example: You have 100 CSR's supporting 100,000 customers; avg. customer acquisition cost is $200; expected lifetime revenue is $1,000 per customer



COMPUWARE®

www.compuware.com