



**EMBARCADERO**  
TECHNOLOGIES

# Auditing Data Access Without Bringing Your Database To Its Knees

Black Hat USA 2006  
August 1-3

**Kimber Spradlin, CISA, CISSP, CPA**  
**Sr. Manager Security Solutions**

**Dale Brocklehurst**  
**Sr. Sales Consultant**

- Auditing Requirements In The Regs
- Accessing Data in the Database
- Native vs. Network Data Access Auditing
- Live Demo



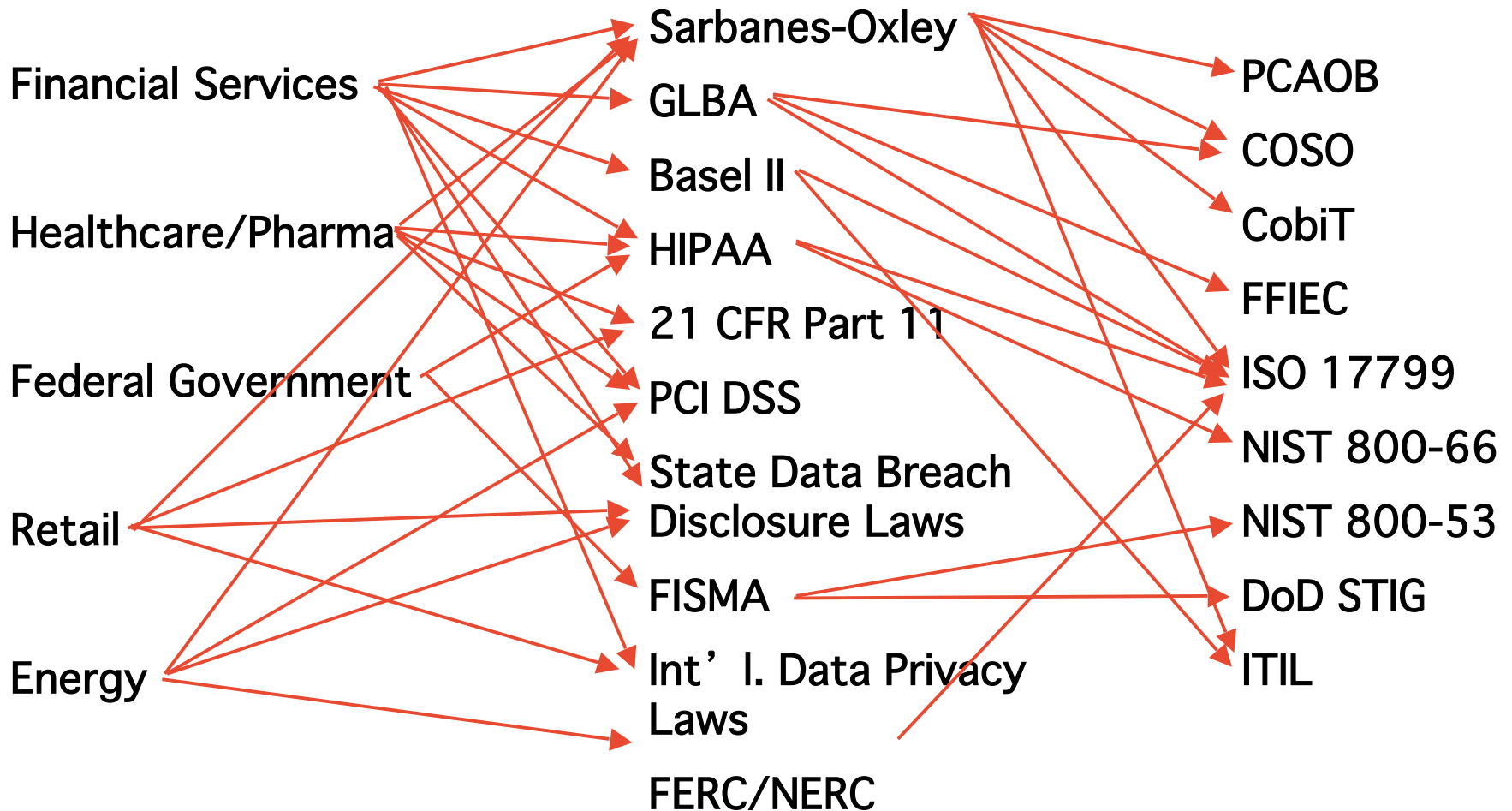
**EMBARCADERO**  
TECHNOLOGIES

# Auditing Requirements In The Regs

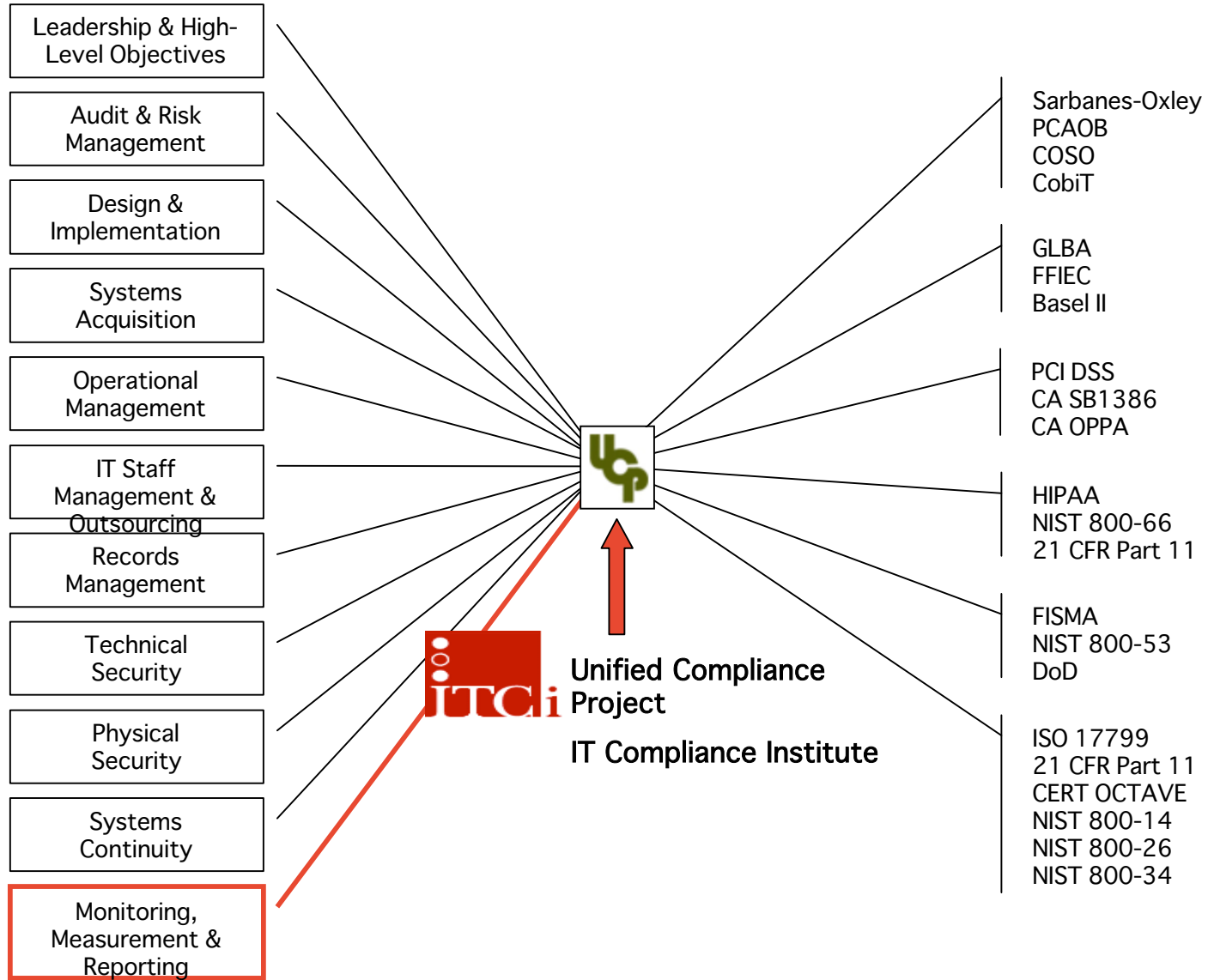
## Industries

## Mandates

## Guidance

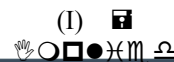


# IT Compliance Clarity



# What to Log

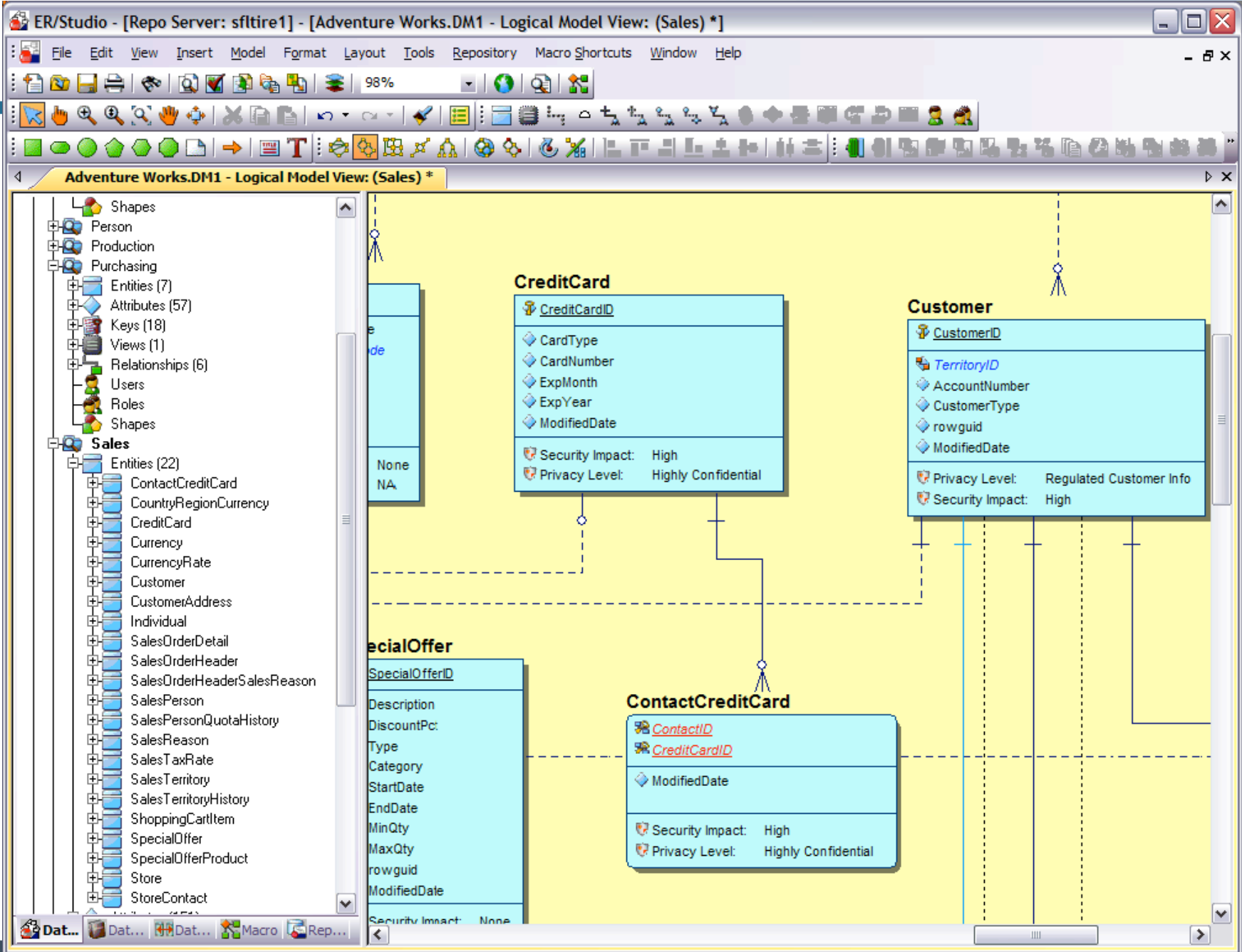
	CobiT (SOX)	PCI DSS	HIPAA	CMS ARS	21 CFR Part 11	GLBA	ISO 17799	NERC	NIST 800-53 (FISMA)
<b>Data Access</b> (Successful/Failed SELECTs)		☺	☺(I)	☺		☺(I)	☺		
<b>Data Changes</b> (Insert, Update, Delete)	☺(I)			☺	☺		☺		
<b>System Access</b> (Successful/Failed Logins; User/Role/Permissions/Pswd changes)	☺(I)	☺	☺	☺	☺(I)	☺	☺	☺(I)	☺
<b>Privileged User Activity</b> (All)	☺(I)	☺	☺(I)	☺	☺(I)	☺	☺	☺(I)	☺(I)
<b>System Changes</b> (Enable/Disable Logs, Services, Configs; Reboots, Errors)	☺(I)	☺	☺(I)	☺	☺(I)	☺(I)	☺	☺(I)	☺(I)
<b>Schema Changes</b> (Create/Drop/Alter Tables, Columns)	☺(I)	☺	☺(I)		☺(I)	☺(I)	☺	☺(I)	☺(I)

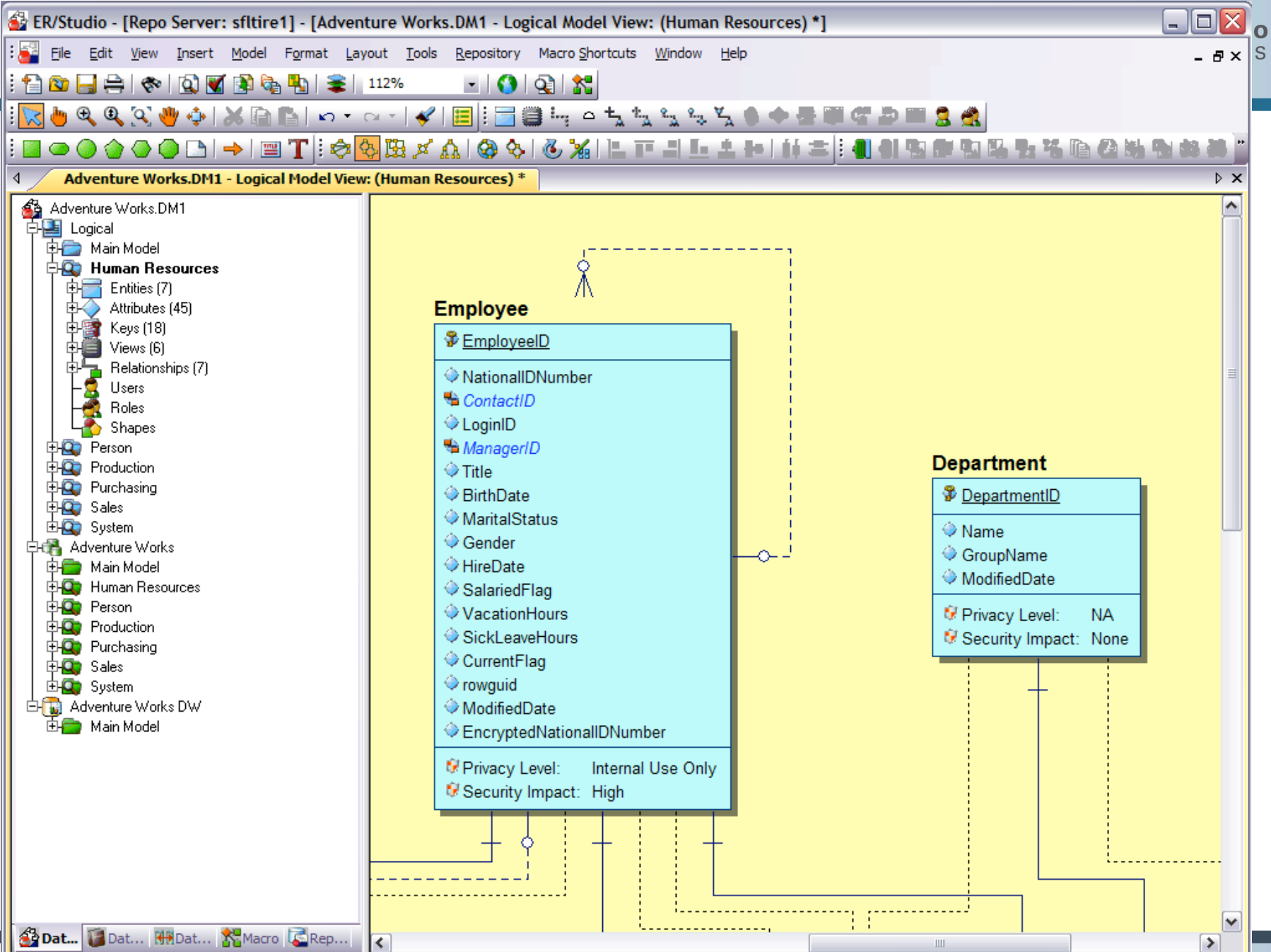
(I) 

- Data Breach Notification Law
- PII = Name + SSN/DL/CC/BA Number
- Specifies notification requirements
  - When – X days after discovery
  - Who – everyone who's data was lost
  - Most offer exemption if data encrypted
  - Some offer exemption if “unlikely” the data will be used
- Does NOT specify how to PREVENT a breach
  - If you aren't monitoring data access, hard to know if there's a breach (except in the case of physical loss)
  - Complete audit trail will give clear picture of exactly what data was taken and which customer records were affected
- **Are you better off not knowing?**
  - “If I don't know a breach occurred then I'm not in violation when I don't notify anyone”
  - Willful ignorance doesn't fly with the regulators
  - Do you really want to learn about the breach from your TV?
  - Tens-of-thousands of customer calls you aren't prepared to handle

- Many locations:
  - E-mail – content security
  - Excel & Word – Help!
  - Paper – physical security
  - **Databases – largest concentration**
- Scan your network!
  - Like all other types of IT assets, you will likely be surprised by how much is out there
  - Must handle devices (e.g. laptops) that aren't always connected to the network
  - Must be able to tell you what applications are installed on each device
  - Must be able to traverse network devices (bridges, routers, firewalls, etc.)
- Tricky part – what kind of data is in those databases you didn't know about?
  - Reverse-engineering tools will build a data model for you
  - Have to gain access to the db first though









**EMBARCADERO**  
TECHNOLOGIES











## Accessing Data in a Database

- Used to retrieve data from the database
- Typically generated by an application and “removed” from the business user
- `SELECT name, address, ssn FROM cust_tbl`
  - Retrieves all records from that table
  - SQL itself does not contain any sensitive data (so neither does the log file)
- `SELECT WHERE acct=1231231123 FROM acct_tbl`
  - Retrieves only one record
  - SQL statement contains account number

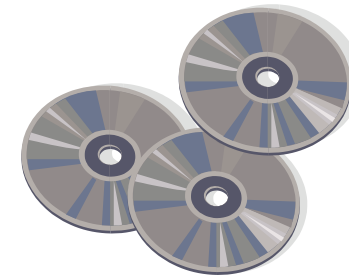
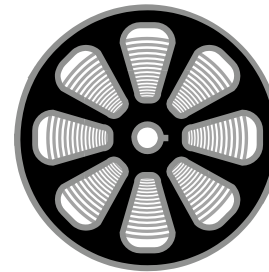
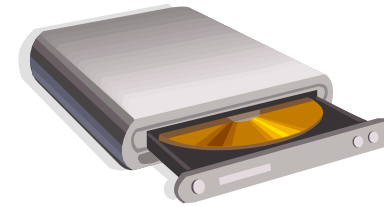
# Protecting Logs

	CobiT (SOX)	PCI DSS	HIPAA	CMS ARS	21 CFR Part 11	GLBA	ISO 17799	NERC	NIST 800-53 (FISMA)
<b>Limit Read Access</b>	☺(I)	☺	☺(I)			☺	☺		
<b>Separate from DBs/ DBAs Being Monitored</b>						☺	☺		
<b>Prevent Changes</b>	☺(I)	☺	☺(I)	☺	☺		☺		☺
<b>Sufficient Storage Capacity</b>	☺(I)		☺(I)			☺	☺		☺
<b>Encrypt Sensitive Data</b>		☺	☺(I)			☺			
<b>Alert on Changes, Capacity, and Errors</b>	☺(I)	☺	☺(I)					☺	☺

(I)   
      

- Additional methods:

- Stored Procedures
- Insert into
- Bulk Copy Programs
- Unload utilities
- Backup routines
- Replication services
- Proprietary APIs



- Watch for:

- Unexpected application IDs
- Unusual syntax
- Unusual source IP

# Review and Retention Requirements

	<b>CobIT (SOX)</b>	<b>PCI DSS</b>	<b>HIPAA</b>	<b>CMS ARS</b>	<b>21 CFR Part 11</b>	<b>GLBA</b>	<b>ISO 17799</b>	<b>NERC</b>	<b>NIST 800-53 (FISMA)</b>
<b>Review Logs Regularly</b>	At least Monthly	Daily	At least Monthly	1-14 Days		Daily	⌘	⌘	⌘
<b>“On-line” Retention</b>	1-7 Years	3+ Month	1 - 6 Years	90 Days	⌘	⌘	⌘	90 Days	⌘
<b>“Off-line” Retention</b>		1+ Years		1 Year					
<b>Back-up Audit Trails To Separate Media</b>	⌘					⌘	⌘		



**EMBARCADERO**  
TECHNOLOGIES

## **Native vs. Network Data Access Auditing**



# Database Auditing Solutions

**Application Users**

Application users login to query and update underlying application data



DML (Insert, Update, Delete)

Enterprise Application

**Privileged Users (DBAs)**



DCL (Grant, Revoke)  
DDL (Create, Drop, Alter)  
DML (Insert, Update, Delete)

(3) Database Auditing

**Corporate Data Assets**

(1) Database Auditing

(2) Database Auditing

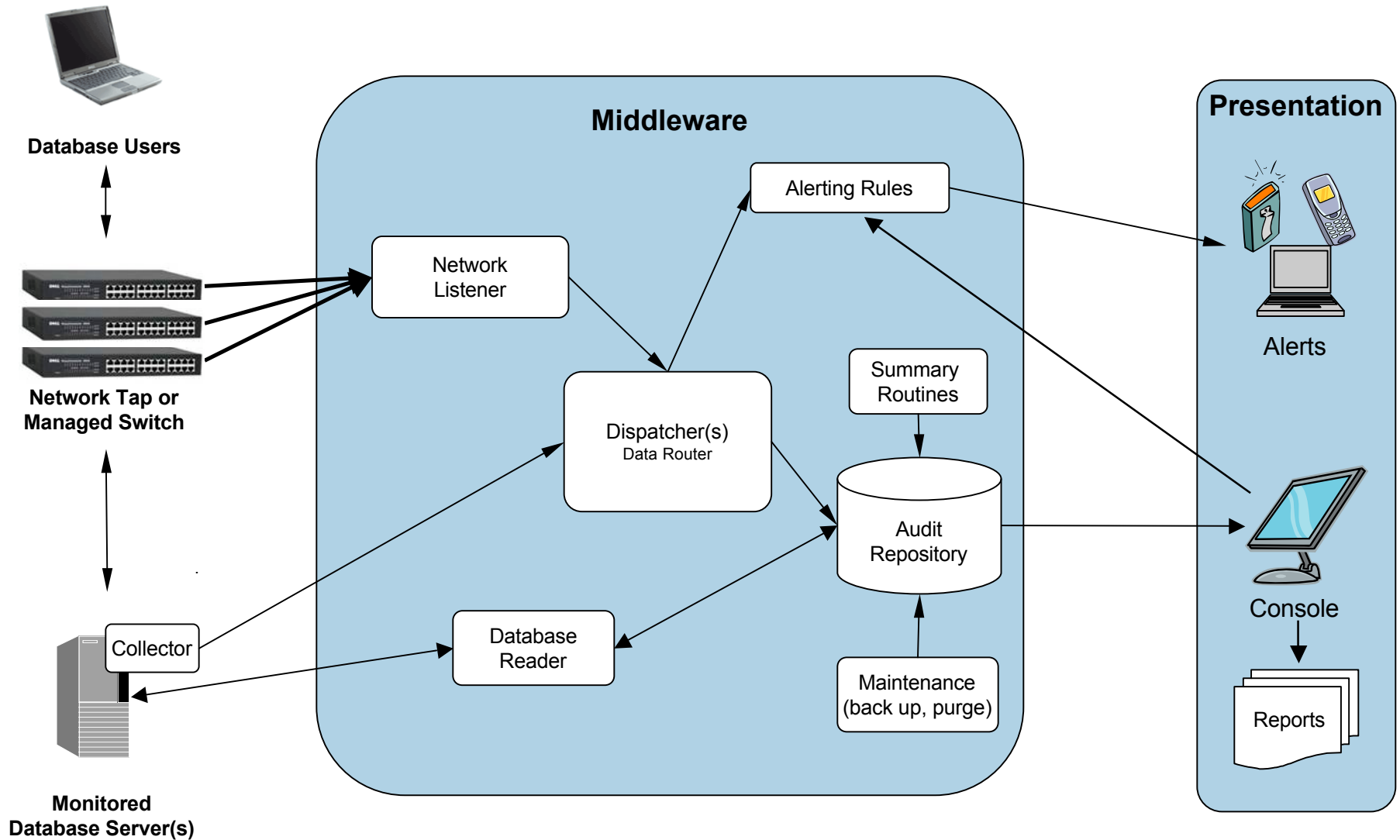
DBAs access and update, accounts, schemas, and data

- **PERFORMANCE!**
  - Data access auditing can significantly slow down existing system performance affecting end-user SLAs
- **Vulnerable to insiders**
  - DB privileged users can disable or alter logs stored on the database being monitored
- **Insufficient visibility, control**
  - Database platforms are highly variable in audit records
- **Complex to manage**
  - Multi-platform environments require multiple skill sets
  - Variable platforms mean inconsistent reports
- **No aggregation**
  - Separate logs for each db instance

Platform	SELECT Auditing
Oracle	Fine Grain Auditing (FGA) – enhanced w/ 10g
Microsoft SQL Server	via SQL Server traces
Sybase	Sp_audit
DB2	Authorization Checking (CHECKING)
Informix	Read Row (RDRW)

- 10-30% CPU impact when enabling logging for all SELECT activity
- Often not granular – must audit a group of activities or audit across all tables
- Full info such as user ID, source IP, table name not always included with the SELECT audit record (just reference numbers that must be looked up)
- Full audit log = stopped database

# Network-based Auditing Architecture



- **Transparency:** no changes to Apps or DBs
- **Completeness:** log everything
- **Performance:** no impact to DBMS performance
- **Availability:** logging failure will not affect DBMS
- **Scalability:** monitor hundreds to thousands of DB instances
- **Segregation of Duties:** remove audit trails from control of systems/users being audited
- **Coverage:** consolidate and analyze across instances and platforms
- **Flexibility:** tailor auditing by activity, table, user, role



**EMBARCADERO**  
TECHNOLOGIES

**Live Demo!**

- Large SELECT statements
- Failed SELECT statements
- Unauthorized source IP
- Unauthorized application ID
- Privileged Users
- Unusual SQL syntax
- Unusual increase in activity
  
- Audience: Others?

- ## Security Benchmarks

- NIST SP 800-70: [http://csrc.nist.gov/checklists/download\\_sp800-70.html](http://csrc.nist.gov/checklists/download_sp800-70.html)
- CIS Configuration Benchmarks: [www.cisecurity.com](http://www.cisecurity.com)
- DISA STIG: <http://iase.disa.mil/stigs/stig/>
- NSA: [http://www.nsa.gov/snac/downloads\\_db.cfm?MenuID=scg10.3.1.2](http://www.nsa.gov/snac/downloads_db.cfm?MenuID=scg10.3.1.2)

- ## Vendor Guidance:

- Oracle: [http://www.oracle.com/technology/pub/articles/nanda\\_fga\\_pt3.html](http://www.oracle.com/technology/pub/articles/nanda_fga_pt3.html)
- MS SQL Server:  
<http://www.microsoft.com/technet/security/prodtech/sqlserver/sql2kaud.msp>
- Sybase: [http://manuals.sybase.com/onlinebooks/group-as/asg1251e/sag/@Generic\\_BookView/39806;td=50#X](http://manuals.sybase.com/onlinebooks/group-as/asg1251e/sag/@Generic_BookView/39806;td=50#X)
- DB2:  
<http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp?topic=/com.ibm.db2.doc.admin/bjndmstr574.htm>
- Informix:  
<http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp?topic=/com.ibm.db2.doc.admin/bjndmstr574.htm>



- [www.embarcadero.com](http://www.embarcadero.com)
- Kimber Spradlin
  - [kimber.spradlin@embarcadero.com](mailto:kimber.spradlin@embarcadero.com)
  - 303-730-7981 x127
- Dale Brocklehurst
  - [dale.brocklehurst@embarcadero.com](mailto:dale.brocklehurst@embarcadero.com)
  - 719-548-7400 x208