Database Auditing: Today's Essential Business Practice for Sarbanes-Oxley Compliance in Year II

Henry Parnell

Entegra Product Strategy

LUMIGENT

Agenda

- Introduction
- SOX Compliance in Year II
- Database auditing – what and why?
- Requirements for a Database Auditing Solution
- Database Auditing Technical Choices
- Entegra
- Summary

What Makes SOX So Different?

- Personal responsibility, liability—internal motivation to act
- Oversight, transparency

  External oversight of public companies by public auditors +
  Aggressive oversight & standards for public auditors =
  Dramatic change in financial reporting and associated processes
- Internal organization re-alignment to underscore independence of audit function
  - Board audit committee structure and function
  - Internal audit (“rock stars” of the corporate world)
- Horizontal applicability to public companies
- SOX is not an event, it is an ongoing process

SOX—Summary Observations (in the first year)

- SOX is real and permanent; an ongoing factor in corporate governance
- Most filers that must file year-end SOX 404 report are focused on big “1st order” issues and activities
  - Minimal effort to comply by 12/31 (stay out of trouble)
  - Activity is/has been focused on:
    - Start-up efforts of education, organization, hiring, training, documentation
    - Highly visible financial-related controls and processes
  - Management, internal and external auditors do not have the time for “2nd order” issues such as IT Controls—need to “pass the test” on 12/31

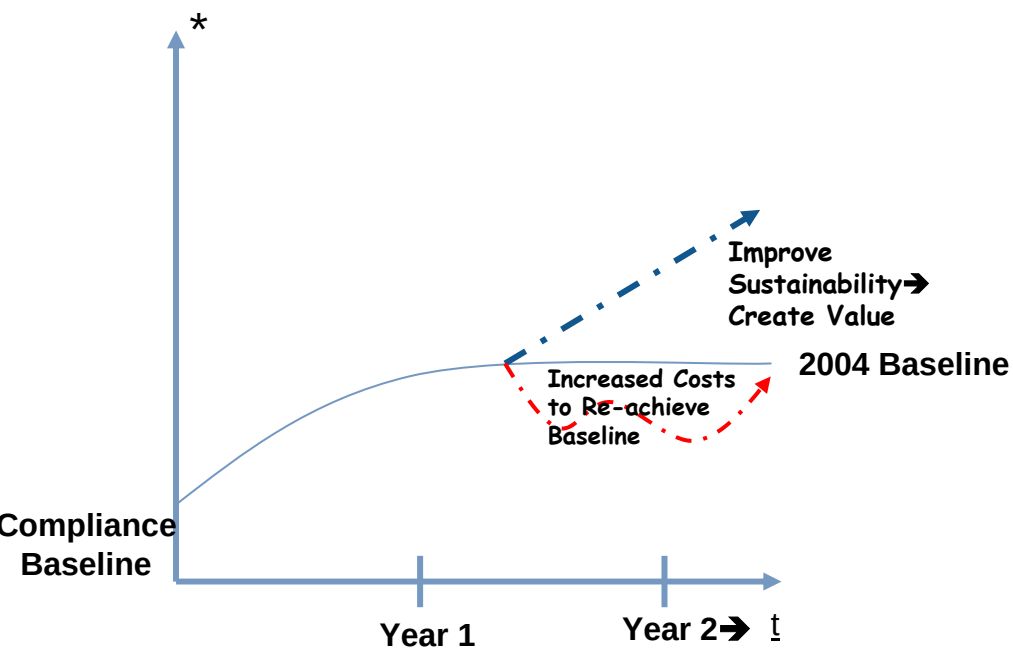
Bottom Line Need to Audit Data

- The DBMS underlying the organization's critical applications holds the crown jewels
- Security to prevent external unauthorized access is insufficient—internal threats to data assets are much more prevalent than external threats
- ***Any*** unmonitored access puts ***all*** data integrity at risk
- Regulatory compliance
  - Management must be able to rely on the integrity of the data in their systems to make regular certifications and assertions
- Best practice
  - Compliance (staying out of trouble) is the minimum effort—data auditing should be an integral IT practice to protect important corporate data assets

Agenda

- Introduction
- SOX Compliance in Year II
- Database auditing – what and why?
- Requirements for a Database Auditing Solution
- Database Auditing Technical Choices
- Entegra
- Summary

State of the Business



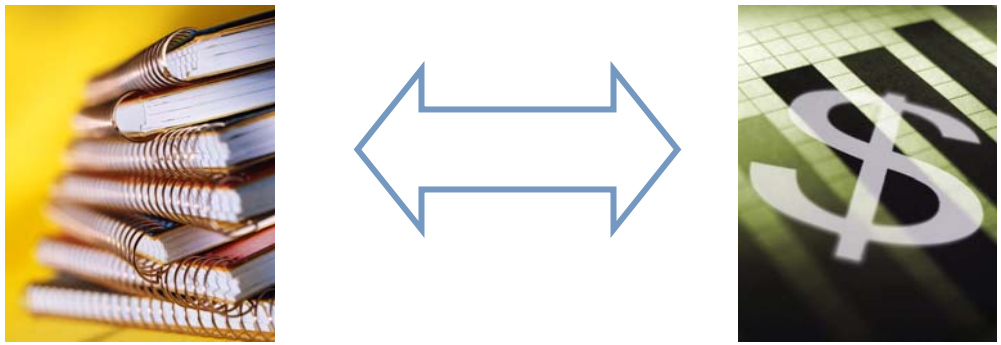
- 2004 Baseline of compliance established
  - Controls identified
  - Weaknesses assessed
- 2005 ?
  - Continual improvement of processes and controls
  - Develop a sustainable compliance cost model
  - Develop a set of analytics on the data collected
  - Compliance ⇔ Risk Management

*Source: Protiviti

LUMIGENT

Transition to Business Value

Coverage **Costs**



- Improve the over-all regulatory infrastructure
- Improve on Year 1 base-line
- Integrate enabling technologies
- Optimize IT infrastructure and reliance on automated controls

Today's Reality: Top 10 Controls Deficiencies*

1. Unidentified or unresolved segregation of duties issues
2. Operating system supporting financial applications not hardened
3. Database management systems supporting financial applications not hardened
4. Development staff can run business transactions in production
5. Large number of users with "super user" permissions
6. Terminated employees or departed consultants still have access
7. Posting periods not restricted within GL application
8. Custom programs, tables & interfaces unsecured
9. Procedures for manual processes do not exist or not followed
10. System documentation does not match actual process

** Joint presentation to ISACA Conference by Audrey Katcher (PricewaterhouseCoopers) & Kenneth Vander Wal (Ernst and Young), April 2004*

Current Thoughts on Costs and Automation (CFO Magazine Feb 2005)

- Total corporate outlays for overall SOX compliance exceeds $6B in 2005 (AMR), mostly for 404 (Foley & Lardner)
  - Large and midsize: $2M annually through 2005 (Gartner)
- US companies with revenues >$5B will spend >$4.6B for 404 compliance (FEI)
- SOX costs expected to rise further before falling
- Micros Systems ($487M) spent $4M over two years on compliance for 404; identified over 1,000 key internal controls.
- Corporate IT manager: >10,000 person-hours preparing systems for 404 compliance → need to move to automation
- Big 4 expected to insist on more automated audit trails

Importance of Data-related IT Controls

- IT systems and data critical to financial reporting process
  - IT controls required because of **pervasive effect on the integrity of data flowing to the financial reports**
  - Financial reports based on data from financial reporting & related business process systems
  - CIOs must build controls that ensure information stands up to audit scrutiny
  - No "single source of truth" for financials – must account for all changes
- PCAOB Auditing Standard No. 2 - importance of IT internal controls

  *"The nature and characteristics of a **company's use of information technology in its information system affect the company's internal control** over financial reporting"*
- Other PCAOB guidance regarding IT controls
  - "…determining which controls should be tested…such controls include… **information technology general controls, on which other controls are dependent"**
  - "Information technology general controls over program development, program changes, computer operations, and **access to programs and data** help ensure that specific controls over the processing of transactions are operating effectively"

Agenda

- Introduction
- SOX Compliance in Year II
- Database auditing – what and why?
- Requirements for a Database Auditing Solution
- Database Auditing Technical Choices
- Entegra
- Summary

Why Database Auditing?

- Standard databases do not keep a complete record of what is happening to them
- Database administrators need to have “privileged access” to database in order to keep them running, make changes, or fix problems
- Overwhelming amount of data and changes make it impossible to distill what is good & what is bad

Because you need to know who is doing what to your data!

Database Auditing Defined

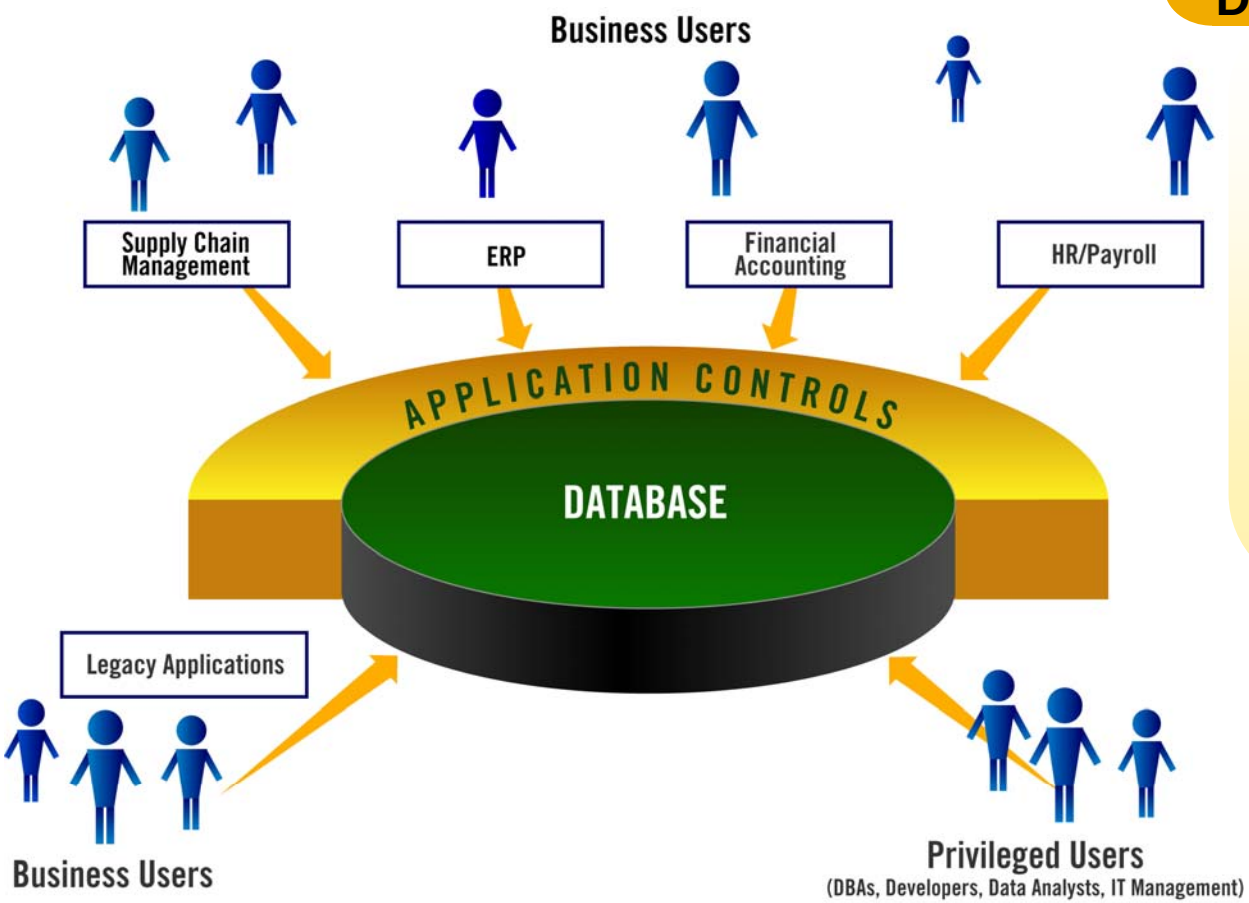
- Auditing isn't new, but database auditing is …
- Ability to continuously monitor, record, & report on all database activity
- A complete audit trail of "*Who did what to which data when and how?*"
- Fundamental drivers for data auditing
  - Business reliance on data systems for operations & financial reporting
  - Increased business risk and regulatory compliance

Data auditing questions

- Who has accessed?
- What have they changed?
- What were the values?
- What did they view?
- Are permissions & changes being tracked?
- Are data structures being altered?
- Are the application controls working as intended?

LUMIGENT

Database Auditing Applies to All Types of Data Access



Data auditing questions

- Who has accessed?
- What have they changed?
- What were the values?
- What did they view?
- Are permissions & changes being tracked?
- Are data structures being altered?
- Are the application controls working as intended?

Any unmonitored activity puts ***all*** data integrity at risk

LUMIGENT

Data Auditing – Why is it Important?

- Integrity of financial reporting
  - *"If all our financial reporting is based on electronically stored data, how can we trust the financial reports without rigorous IT controls and monitoring?*

    William Powers, Associate Director, PCAOB
    Keynote presentation at ISACA Symposium "SOX: A Focus on IT Controls", Apr 2004
- Operational imperative to manage and control risk
  - Every aspect of modern enterprise dependent upon application and data systems
  - Protection of critical and sensitive corporate assets
- Regulatory compliance
  - International, Federal, State regulations demand controls to ensure data integrity and privacy (SOX, Basel II, SB1386, …)
- Capital market expectations of transparency
  - Audit deficiencies can impact corporate credit rating (ex: Moody's)

Examples of Legislative Requirements

- Sarbanes-Oxley Act
  - CEO / CFOs must evaluate and report on the effectiveness of internal controls over financial reporting
  - Requires a comprehensive data audit to show that data has not been comprised
- HIPAA
  - Assures protection of patient health information
  - Requires that a corporation show how data records are accessed and by whom
- Graham Leach-Billery Act and Basel II
  - Protects the confidentially of personal financial information
  - Corporations must show how data records are accessed and by whom
- Many of the regulations require data retention
  - Seven or more years is typical

Data Auditing for Sarbanes-Oxley

SOX Requirement	Database Auditing
Veracity of financial reporting	▪ Who accessed what data? ▪ What have they changed? ▪ What were the values? ▪ What did they view?
Reporting and effectiveness of internal controls	▪ Are application controls working as intended? ▪ What's happened to the underlying data? ▪ Were data structures or permissions altered?

Auditing the **database** is the *last line of defense* and a *true record* of what happened.

LUMIGENT

Business Impact of Improper Database Access and Use

Threat	Negative Impact	Example Business Impact
Privileged user makes unauthorized data changes	Company is now operating against false data	CFO attests to falsified financial data
Privileged user makes unauthorized permissions changes	Enables fraudulent, untraceable data tampering	User accesses compensation & health records, violating company privacy commitments
Privileged user views records without authorization	User now has access to data against policy	User accesses customer-personal information, violating SB1386 – company must notify all customers
User modifies financial transaction data “by hand” without approval	Improper financial transaction execution	Company fails SEC audit, resulting in penalties; company fails “best execution” test, resulting in fines
User runs rogue transaction process	Financial fraud	User siphons off millions of dollars from transaction flow
User views customer-personal information	Identity theft, financial fraud	Allows intruder to transfer customer funds without approval
User runs rogue data-collecting SQL queries	Leakage of corporate proprietary information	Get list of customer accounts
Fraud without audit trail	Lack of evidentiary trail	Punitive actions by FBI, failed litigation

Improper Database Access Means Risk

"If all our financial reporting is based on electronically stored data, how can we trust the financial reports without rigorous IT controls and monitoring?

William Powers, Associate Director, PCAOB
Keynote presentation at ISACA Symposium "SOX: A Focus on IT Controls", Apr 2004

- Insiders with legitimate privileges can change or view data improperly
- Insiders without privileges can exploit bad security policies to change or view data improperly
- Outsiders can exploit vulnerabilities to violate access policies

Any one of these can result in serious and real business consequences.
"Trust but verify" – "Trust" alone just *increases* risk

Agenda

- Introduction
- SOX Compliance in Year II
- Data auditing – what and why?
- Requirements for a Database Auditing Solution
- Database Auditing Technical Choices
- Entegra
- Summary

Enterprise Database Auditing Requirements

Trusted

- Unimpeachable audit trail
- Meets audit requirements
- Segregation of duties
- Separation of audit system
- Audits privileged users
- Comprehensive
- Modifications
- Structure
- Views*

Deliver Business Value

- Reporting
- Analytics
- Alerting for risk management
- Complete record for regulatory compliance
- Augments security measures

Enterprise Enabled

- Minimal performance impact
- Seamless, non-disruptive integration with current operations
- Supports multiple platforms
- Ease of administration for maximum efficiencies, productivity

Examples of specific requirement

Capture all relevant database activity in a usable format to allow:

- Continuous monitoring of all privileged user access
- Forensic support for current application and IT-dependent controls
- Primary control where automated IT control not possible
- Backstop when the need for control has not been anticipated

Augmentation of IT security/access controls for critical database resources

- Immediate notification of user ID and user privileges/roles changes
- Permanent audit trail of event to repository
- Compare event to approved baseline of users/privileges and change control approvals - Vulnerability assessment

Examples of specific requirement

- Continuous monitoring of **all** activity that falls outside of the application or other controlled space
  - All metadata (infrastructure), user ID, and user privilege changes
  - All database content changes (inserts, deletes, modifications) from outside an application
  - All data viewing activity (privacy concerns, data theft, inappropriate data viewing) from outside an application

Worst Case Requirement

Comprehensive Risk Mitigation

- Provide assurance of use and access to data, including by DBA staff
- Mitigate risk of ambiguous regulatory requirements with a complete audit trail of **all** database activity
- Assurance that data assets are used and accessed appropriately, data is correct, and security policies work

Agenda

- Introduction
- SOX Compliance in Year II
- Data auditing – what and why?
- Requirements for a Database Auditing Solution
- Database Auditing Technical Choices
- Entegra
- Summary

Implementing Audit

- Network Layer
  - Packet sniffing
- Mid-tier or application layer
  - Application maintains an audit trail
- In the Database
  - Triggers
  - Native DB Tools
    - Oracle Audit
    - Log Miner Products
  - Transaction log

Network Layer

- Packet sniffing (gateway or host)
  - Big back door
    - A user can log directly to the database, bypassing audit
  - May be encrypted
    - Content is inaccessible
  - Incomplete
    - No access to before after/values
    - No visibility into actions of a stored procedure
  - Requires heavy-duty reverse engineering of protocol

Mid-Tier, Application Layer

- Application modification
  - No visibility into actions of a stored procedure
  - Difficult to retrofit into legacy applications
  - Expensive to build and maintain
  - Does not audit DBAs, privileged users
  - Requires modification of every application
    - Costly, labor-intensive
    - Not possible for 3rd party applications
  - Doesn’t account for direct database access

In the Database Alternatives – What to instrument for collection?

- Triggers - Database
  - Can be difficult to create, manage and maintain
  - Impact on performance!
  - Incomplete: before and after data values, changes to schema
  - No support for multiple platforms applications
  - Unable to capture changes to database permissions and schema

In the Database Alternatives – What to instrument for collection?

- Native built-in audit - Database
  - Incomplete, doesn't cover all operations
  - Performance/storage intensive
  - Fails separation of duties, DBA Security Tool
  - Just captures DDL, access control, permission
  - No included aggregation, reporting, analytics
  - Not a multi-DBMS, enterprise-wide solution
- Log Reading - Database
  - Incomplete, doesn't cover Selects
  - Fire Hose of data
  - Can have separation of duties problems
  - small performance impact!

Agenda

- Introduction
- Compliance in Year Two
- Data auditing – what and why?
- Requirements for a Database Auditing Solution
- Database Auditing Technical Choices
- Entegra
- Summary

Lumigent Technologies, Inc.

- Mission – **mitigate risk associated with data access and use** by:
  - Assuring integrity of all critical data assets
  - Addressing regulatory requirements for data integrity, privacy, and security
- Founded December 1999
- 2,200+ corporate customers

Microsoft GOLD CERTIFIED Partner

ORACLE PARTNERNETWORK

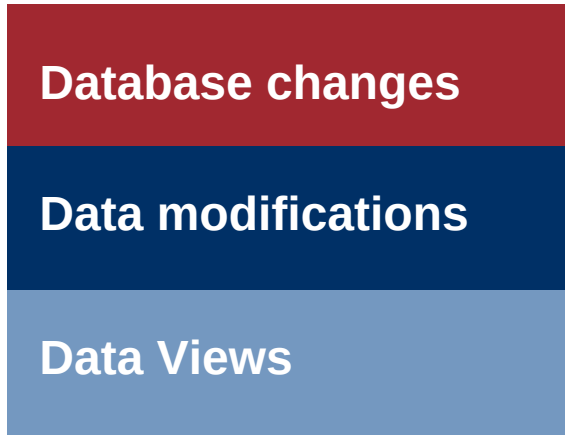
SYBASE

Introducing Entegra

- A comprehensive auditing solution that mitigates business risk with insight into how enterprise data is used, for:
  - Regulatory compliance (SOX, HIPAA, EUDPA, GLBA…)
  - Internal requirements for data security and privacy
  - Protection of sensitive data assets
  - Customer and partner confidence
  - Data center / operational requirements for auditing

Key Capabilities

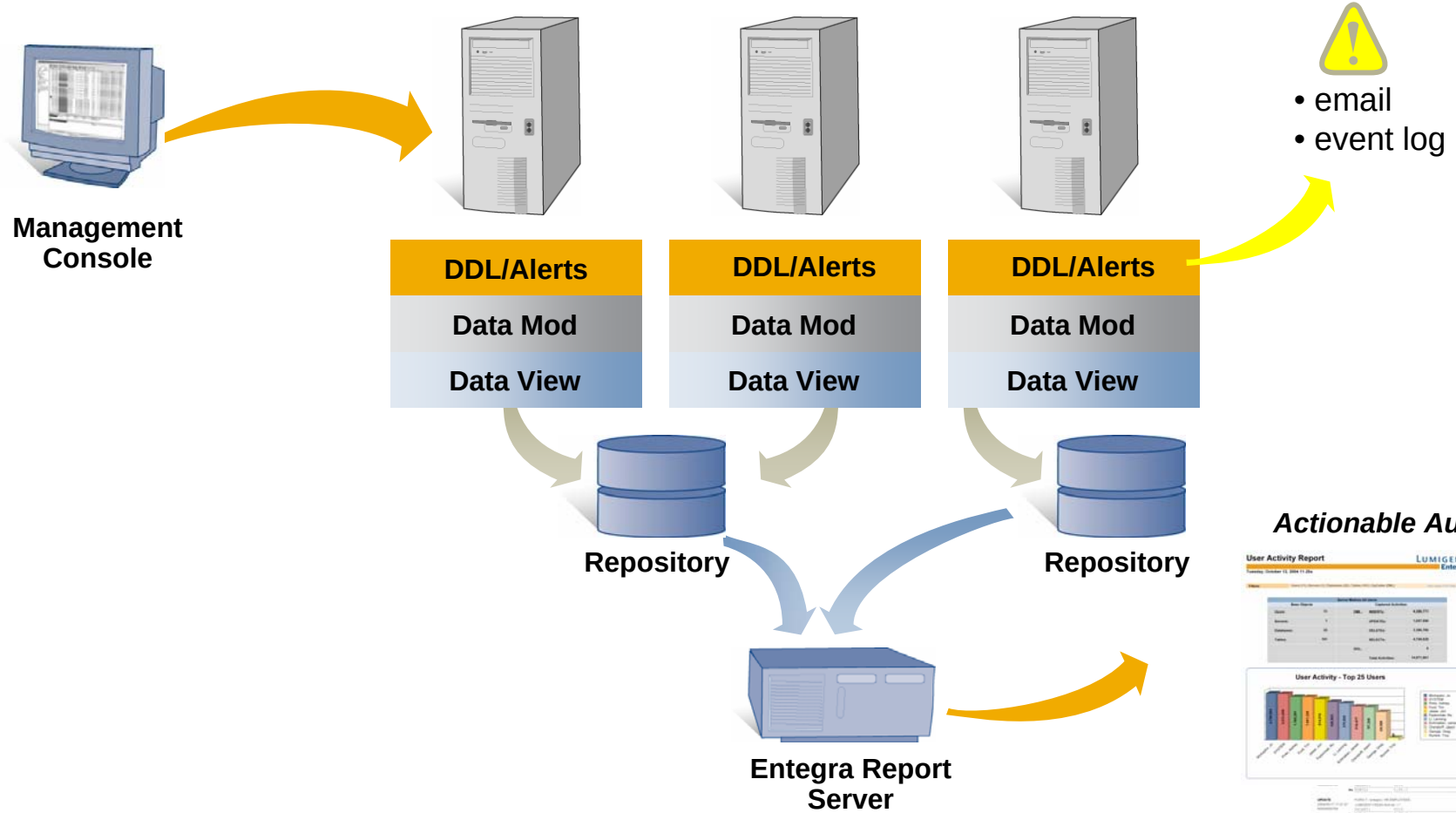
- Audit trail of data activity on multiple servers
  - Changes to database schema and permissions (DDL), logins
  - Data changes (DML activity)
  - Data Views (Selects)
- Shared repository for archival storage
  - Centralized data collection
  - Independent of audited servers
  - Consolidation of data for ease of reporting
  - Long-term archival management
- Support
  - MS SQL-Server, Oracle, Sybase ASE, (upcoming UDB/DB2)
  - Across all major OS platforms



Features of the Entegra Auditing System

- Centralized audit data repository
- Easy to use interface for setup and configuration
- Notification when schema or permissions are changed
- Record of all schema and permission changes
- Identifies what data was changed, when and by who
- Identifies who viewed certain data and when
- Generates usage reports on who accessed certain data
- Enables investigation of suspicious behavior
- Tracks who modified what over a given time period
- Automates the auditing process across the enterprise

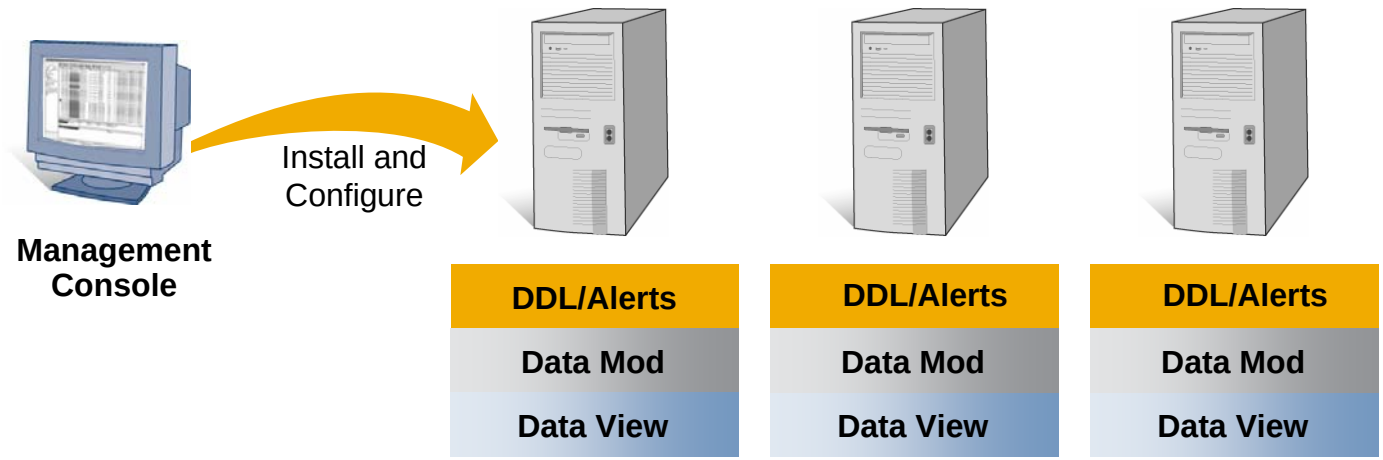
Entegra: Enterprise Architecture



Actionable Audit Trail!

LUMIGENT

Entegra: Enterprise Architecture



Data Definition Module (DDL)

- Audit of DDL and security changes
- Real-time alerts to email & event log

Data Modification Module (DML)

- Capture DB content changes
- Specify DB, table, column to audit

Data View Module (SELECTS)

- Capture data viewing events
- Specify DB, table to audit

Entegra Architecture in 4 Stages

Management Console

Target Audit Databases

Stage 1 Configuration

Stage 2 Collection

Entegra Repository

Stage 3 Loading Repository

Stage 4 Reporting

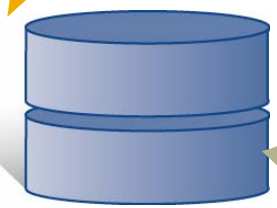
Entegra Report Server

Actionable Audit Trail!

Stage 1 Configuration

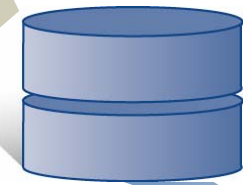
Management Console

Target Audit Database



- Install collection modules
- Configure modules: DDL, DML, SELECTs
- Set schedule for collection
- Set alerting parameters

Entegra Repository



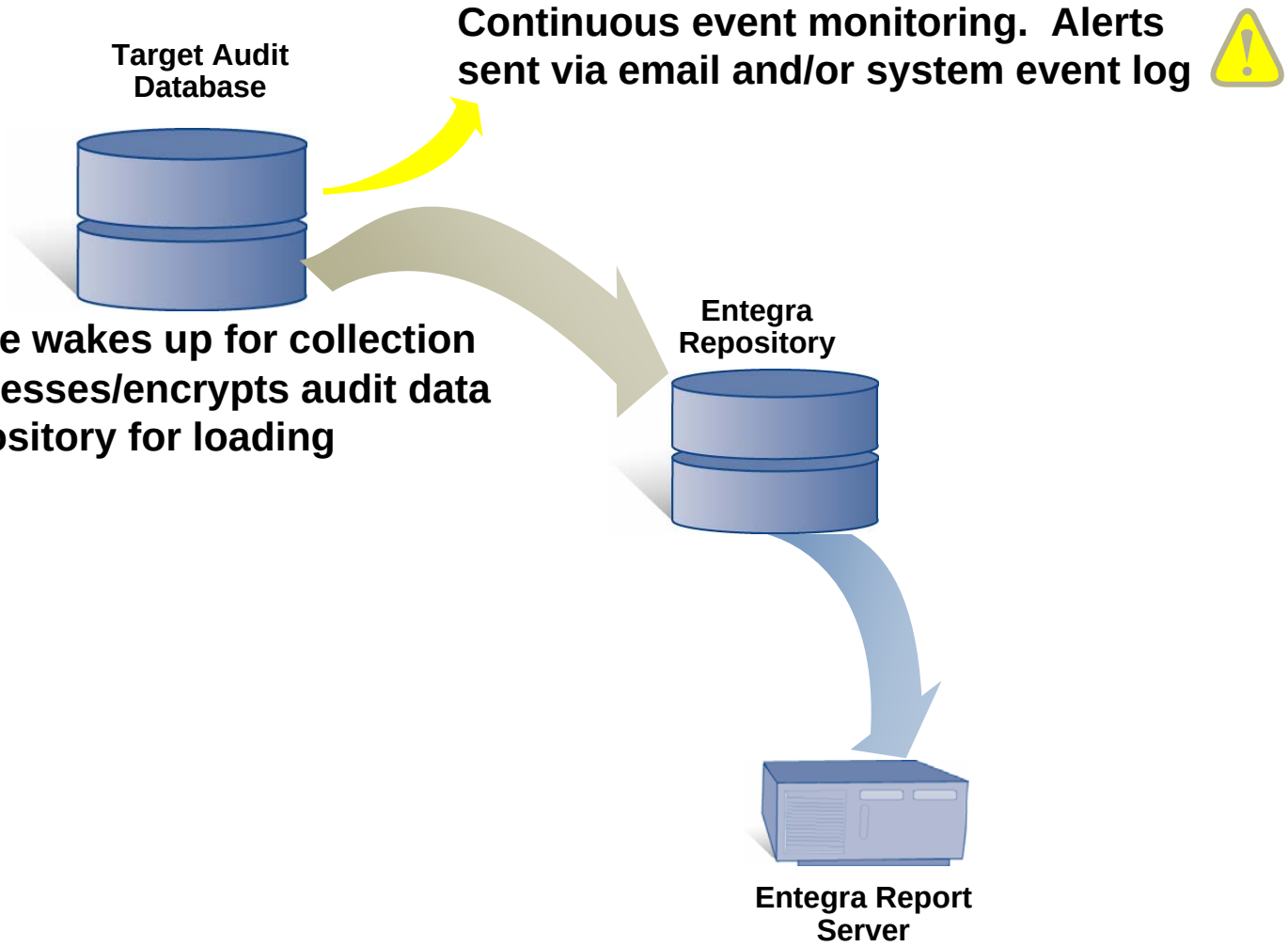
- Create repository schema
- Configure repository settings
- Set archiving/purging

Entegra Report Server

- Install report server
- Configure report users
- Set report parameters
- Set reporting schedule

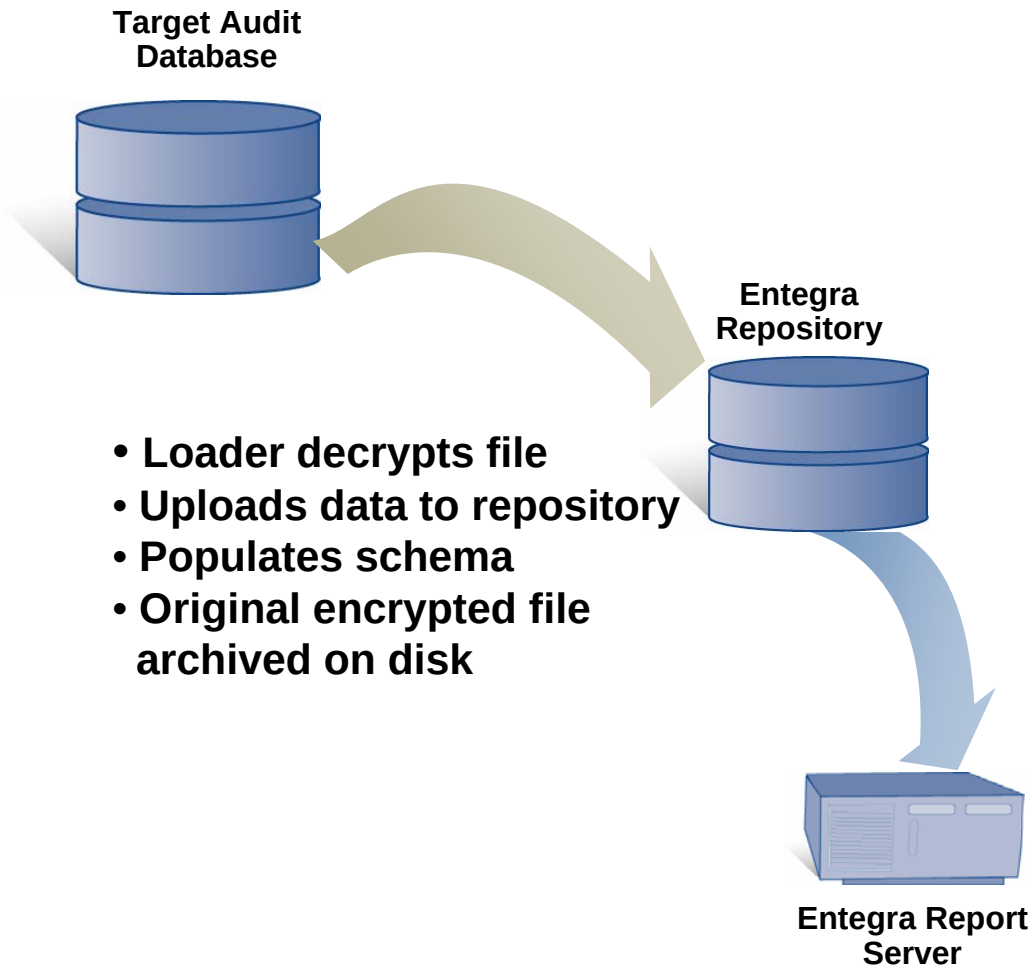
LUMIGENT

Stage 2 Collection

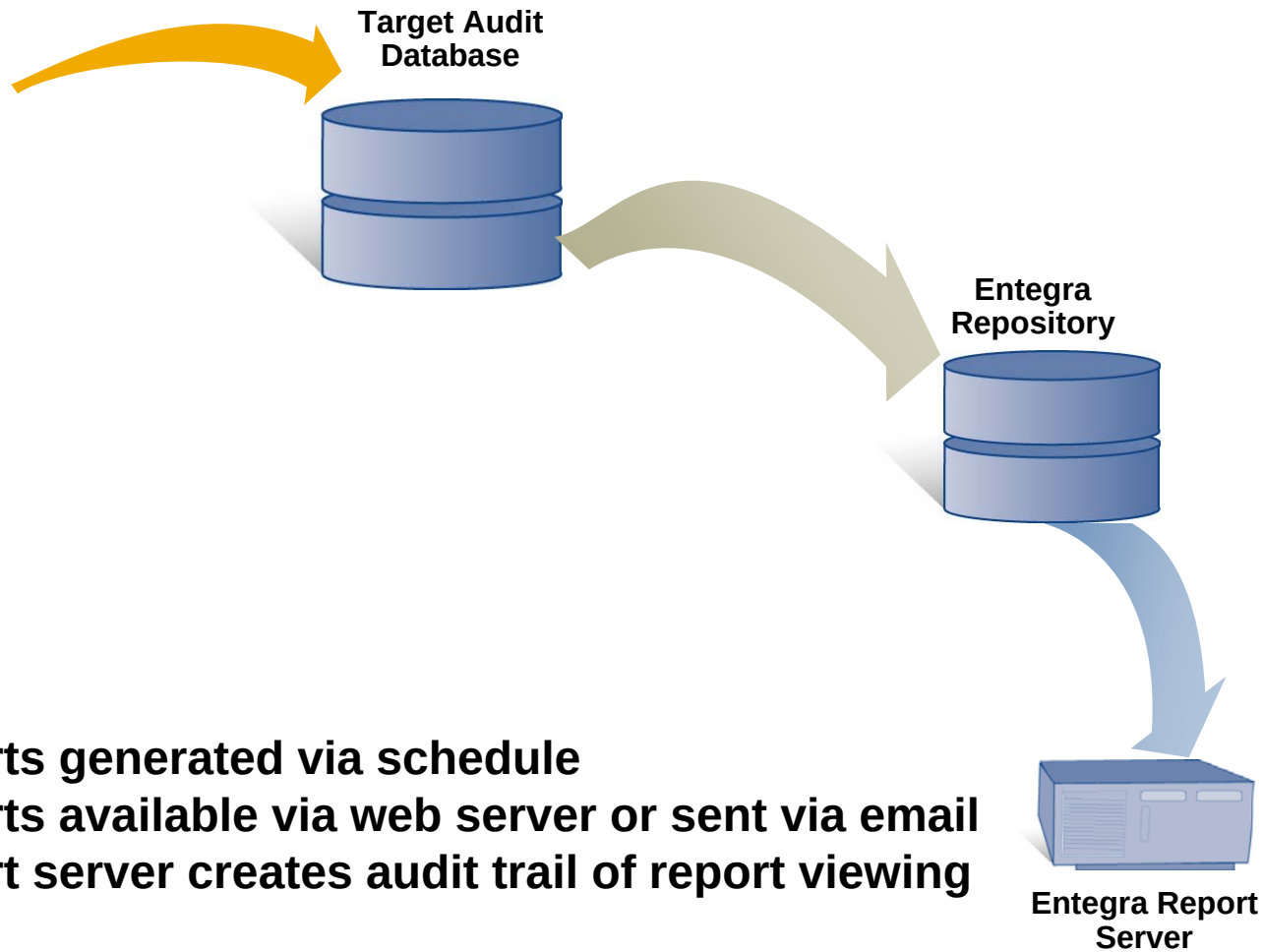


- Collection module wakes up for collection
- Takes and compresses/encrypts audit data
- Sends file to repository for loading

Stage 3 Loading Repository



Stage 4 Reporting



- Reports generated via schedule
- Reports available via web server or sent via email
- Report server creates audit trail of report viewing history

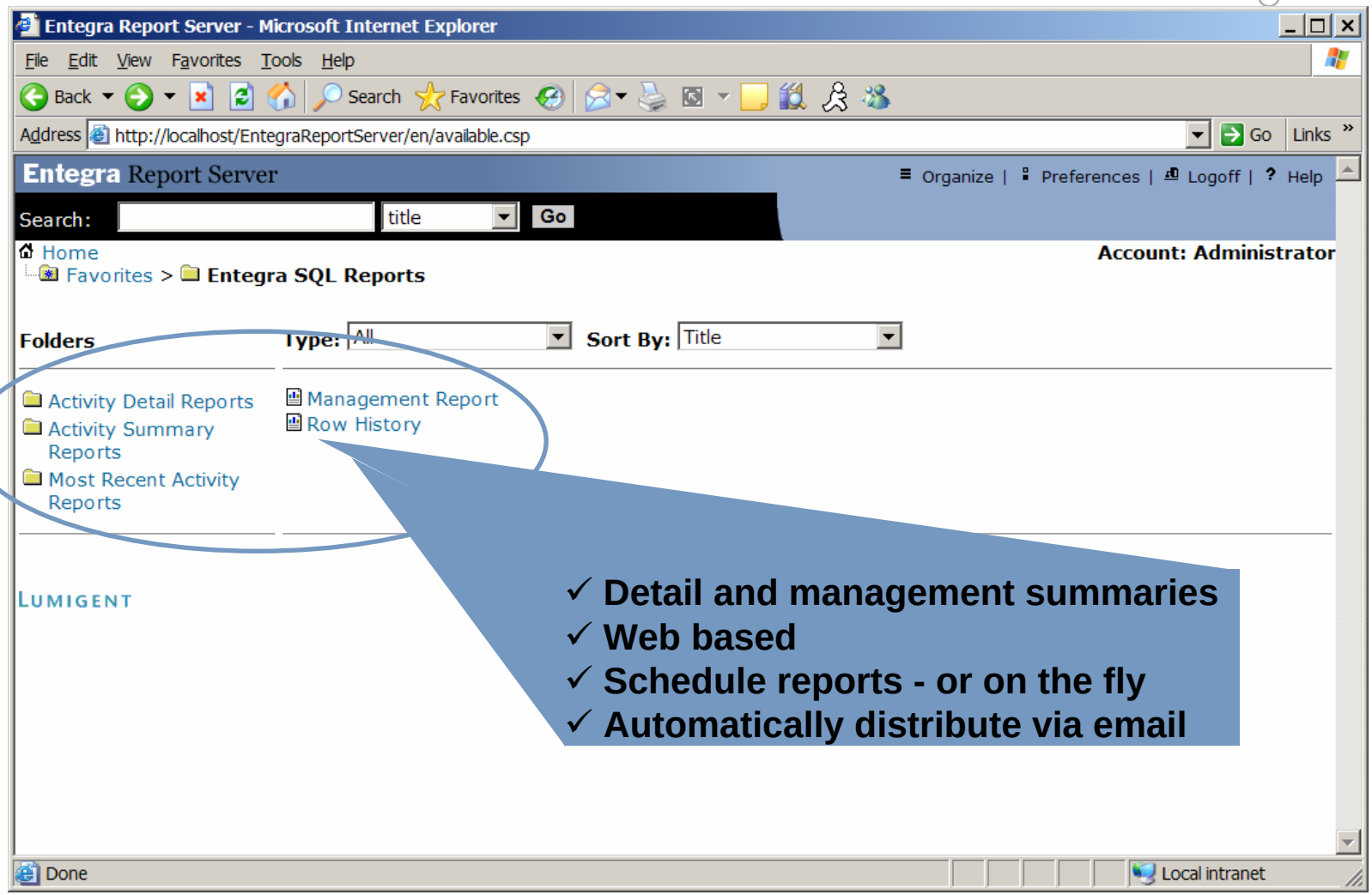
LUMIGENT

Entegra : Reporting Features

- Provides powerful reporting on repository data
  - Multiple formats: PDF, MS Word, MS Excel, HTML
  - View online or send via email
  - Schedulable: Monthly, Weekly, Daily, Hourly
  - Access protected
- Includes 25 standard reports
  - 12 Activity Summary Reports
    - Most Recent Activity & Search on Data Value
  - 12 Activity Detail Reports
  - 1 Row History Report
- Meets enterprise reporting needs
  - IT audit and compliance
  - Database operations
  - Security & forensics

LUMIGENT

Entegra: Reporting



Know What is Happening to Your Database

Activity Summary Report

LUMIGENT Entegra

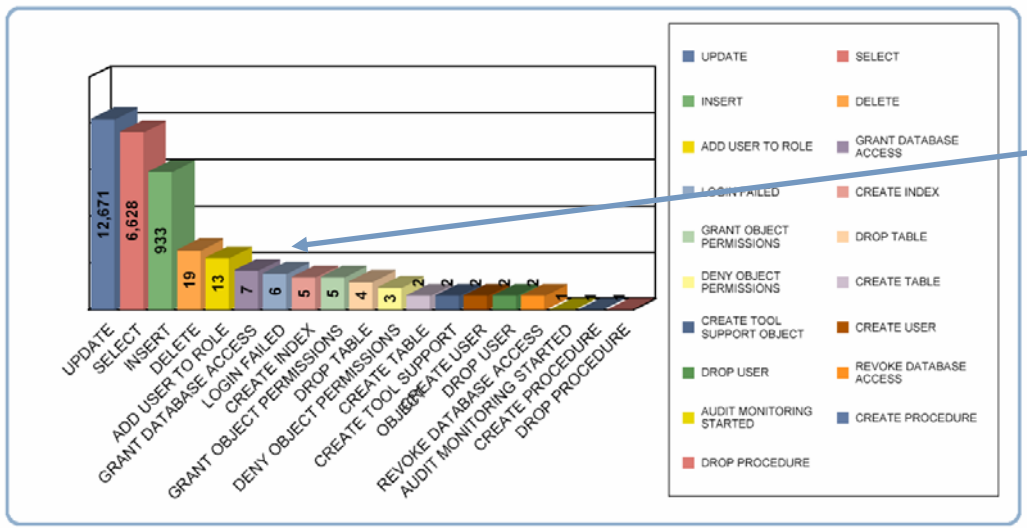
Thursday, December 2, 2004 1:51p

Filters: Users (All) | Servers (All) | Databases (All) | Tables (All) | OpCodes (All) See page 2 for filter details

Server Metrics All Users				
Base Objects		**Captured Activities:**		
Users:	6	DML:	INSERTs:	933
Servers:	1		UPDATEs:	12,671
Databases:	1		DELETEs:	19
Tables:	6	SELECTs:		6,628
		DDL:		56
			Total Activities:	20,307

Aggregated Summary of all activity

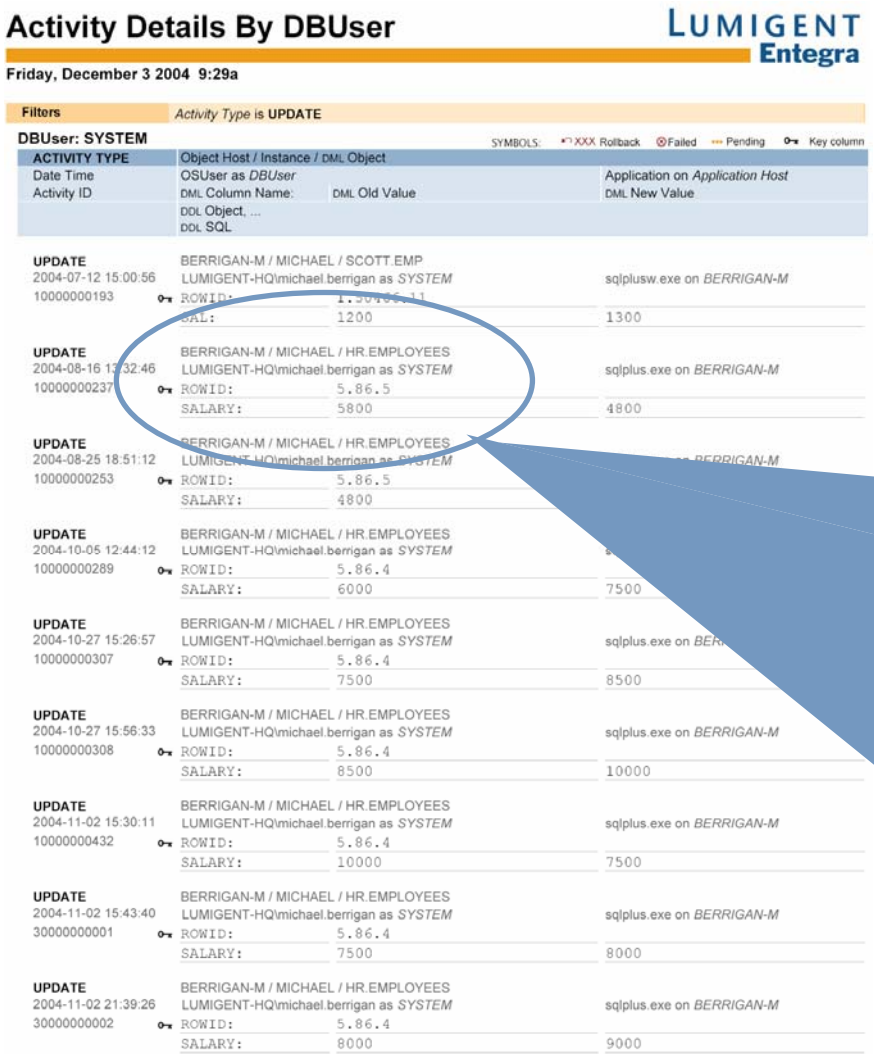
Activities - Top 25 Activity Types



Drill Down on specific activity

LUMIGENT

In Depth, Complete Record of Changes



Activity Details By DBUser

LUMIGENT Entegra

Friday, December 3 2004 9:29a

Filters *Activity Type* is **UPDATE**

DBUser: SYSTEM

SYMBOLS: XXX Rollback ⊗Failed ••• Pending Key column

ACTIVITY TYPE	Object Host / Instance / DML Object		
Date Time	OSUser as *DBUser*		Application on *Application Host*
Activity ID	DML Column Name:	DML Old Value	DML New Value
	DDL Object, ...		
	DDL SQL		
UPDATE	BERRIGAN-M / MICHAEL / SCOTT.EMP		
2004-07-12 15:00:56	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplusw.exe on *BERRIGAN-M*
10000000193	ROWID:	[illegible]	
	SAL:	1200	1300
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-08-16 13:32:46	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplus.exe on *BERRIGAN-M*
10000000237	ROWID:	5.86.5	
	SALARY:	5800	4800
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-08-25 18:51:12	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		on *BERRIGAN-M*
10000000253	ROWID:	5.86.5	
	SALARY:	4800	
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-10-05 12:44:12	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		
10000000289	ROWID:	5.86.4	
	SALARY:	6000	7500
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-10-27 15:26:57	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplus.exe on *BER*
10000000307	ROWID:	5.86.4	
	SALARY:	7500	8500
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-10-27 15:56:33	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplus.exe on *BERRIGAN-M*
10000000308	ROWID:	5.86.4	
	SALARY:	8500	10000
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-11-02 15:30:11	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplus.exe on *BERRIGAN-M*
10000000432	ROWID:	5.86.4	
	SALARY:	10000	7500
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-11-02 15:43:40	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplus.exe on *BERRIGAN-M*
30000000001	ROWID:	5.86.4	
	SALARY:	7500	8000
UPDATE	BERRIGAN-M / MICHAEL / HR.EMPLOYEES		
2004-11-02 21:39:26	LUMIGENT-HQ\michael.berrigan as *SYSTEM*		sqlplus.exe on *BERRIGAN-M*
30000000002	ROWID:	5.86.4	
	SALARY:	8000	9000

- ✓ **Who made what change when**
- ✓ **Before and after values**
- ✓ **Actual row affected**

LUMIGENT

See All Changes to a Specific Row

Row History

LUMIGENT Entegra

Wednesday, December 1 2004 4:20p

FILTERS	*Key Value* like **OLDWO**

Object Host / Instance / Object

HERMAN-E / HERMAN-E / EntegraDemoDB.dbo.Customers

SYMBOLS: XXX Rollback Failed Pending Key column

ACTIVITY	OSUser as *DBUser*		Application on *Application Host*
Date Time	Column Name	Old Value	New Value
Activity ID			

ACTIVITIES FOR KEY

Column Name	Value
CustomerID:	OLDWO

UPDATE 2004-11-22 10:58:17 13575	DeptMgr as *HERMAN-E\DeptMgr* Phone:	(907) 555-7584	DemoApp on *HERMAN-E* 555-555-1111
UPDATE 2004-11-22 10:58:20 13530	DeptMgr as *HERMAN-E\DeptMgr* CompanyName:	Old World Delicatessen	DemoApp on *HERMAN-E* Old World Deli
UPDATE 2004-11-22 10:58:20 13527	DeptMgr as *HERMAN-E\DeptMgr* ContactName: ContactTitle:	Rene Phillips-Jones Senior Account Manager	DemoApp on *HERMAN-E* Eric Herman Account Manager
UPDATE 2004-11-22 10:58:20 13528	DeptMgr as *HERMAN-E\DeptMgr* ContactTitle:	Account Manager	DemoApp on *HERMAN-E* Senior Account Manager
UPDATE 2004-11-22 10:58:20 13529	DeptMgr as *HERMAN-E\DeptMgr* ContactName: ContactTitle:	Rene Phillips Sales Representative	DemoApp on *HERMAN-E* Rene Phillips-Jones Account Manager
UPDATE 2004-11-22 10:58:20 13526	DeptMgr as *HERMAN-E\DeptMgr* Address: City: PostalCode:	2743 Bering St. Anchorage 99508	DemoApp on *HERMAN-E* 9 Juniper Lane Nome 99552

Transaction history for unique row

LUMIGENT

Data Auditing Scenario #1

Situation	• Privileged db user making changes to critical database: (1) objects/schemas, (2) db IDs and privileges
Need	• Reconcile all changes against change mgmt system to confirm: - Change was authorized - Results are as intended
Implications	• Lack of privileged user activity audit trail is an unacceptable business risk and may render other controls ineffective
Challenges	• Privileged users need complete access to perform duties • Piecemeal or labor intensive manual approaches may lack in completeness or fail to be executed • Platform tools (e.g. triggers) incomplete; introduce performance & resource issues; lack consolidation, reporting & mgmt capabilities
Sybase Audit Solution	• Continuous audit trail of all changes at the database level - enterprise-wide consolidation to central repository - schedulable, customized reporting • Improved efficiency, accuracy, time to report

Report Example – Change to Stored Procedure Underlying Critical HR App

Activity Details

LUMIGENT

SYMBOLS: XXX Rollback | Failed | Pending | Key column

ACTIVITY TYPE	Object Host / Instance / DML Object		
Date Time Activity ID	OSUser as *DBUser* DML Column Name:	DML Old Value	Application on *Application Host* DML New Value
	DDL Object, ... DDL SQL		
DROP PROCEDURE 2005-01-19 15:44:34 15009	HERMAN-E / HERMAN-E eric.herman as *Intruder*		lumsql on *HERMAN-E*
	`drop procedure sp_add_employee`		
CREATE PROCEDURE 2005-01-19 15:44:34 15010	HERMAN-E / HERMAN-E eric.herman as *Intruder*		lumsql on *HERMAN-E*
	`create procedure sp_add_employee as DELETE [EntegraDemoDB].[dbo].[Employees] WHERE EmployeeID=2; INSERT INTO [EntegraDemoDB].[dbo].[Employees] ([EmployeeID], [LastName], [FirstName], [Title], [TitleOfCourtesy], [BirthDate], [HireDate], [Address], [City], [Region], [PostalCode], [Country], [SSNumber], [AnnSalary], [HomePhone], [Extension], [ReportsTo]) VALUES (2, 'Theboss', 'I.M.', 'VP Worldwide Sales', 'The Man', '1970-02-19 00:00:00.000','1990-01-22 00:00:00.000', '55 Living Large Way', 'Seattle', 'WA', '15604', 'USA', '555555555', 1000000.0000, '(206) 555-1212', 2600, '1')`		

LUMIGENT

Report Example—User ID Granted Privileges to an Existing Database

Activity Details

LUMIGENT

SYMBOLS: ↶XXX Rollback ⊗Failed ••• Pending 🔑 Key column

ACTIVITY TYPE	Object Host / Instance / DML Object		
Date Time Activity ID	OSUser as *DBUser* DML Column Name:	DML Old Value	Application on *Application Host* DML New Value
	DDL Object, ... DDL SQL		
DROP TABLE 2005-01-19 15:44:15 15005	HERMAN-E / HERMAN-E ElaineT as *sa* DROP TABLE suppliers		lumsql on *HERMAN-E*
GRANT DATABASE ACCESS 2005-01-19 15:44:33 15006	HERMAN-E / HERMAN-E eric.herman as *Intruder* The user sa executed the sp_grantdbaccess procedure in the "EntegraDemoDB" database on HERMAN-E. sp_grantdbaccess is used to grant a login access to a database. In this case, the login "Intruder" was specified as the login to be granted access to the database "EntegraDemoDB". The user sa was logged in via an application that identified itself as "lumsql" from the computer HERMAN-E.		lumsql on *HERMAN-E*

LUMIGENT

Data Auditing Scenario #2

Situation	• Critical legacy application determined to have inadequate logging function of user activity
Need	• Implement cost-effective user logging without resorting to costly code modifications or application replacement
Implications	• Could result in a material weakness and/or expose the business to operational unacceptable risk • Attempts to modify application may be deemed too costly or introduce risk in the stability of a critical application
Challenges	• Overcoming build (vs. buy) mentality of internal IT staff
Sybase Audit Solution	• Continuous audit trail of all changes at the db level • Log and exception reports to support key controls • Rapid low-cost implementation without risk to app stability

Example: Unauthorized Changes to Legacy Commission System

Activity Details

LUMIGENT

SYMBOLS: XXX Rollback ⊗Failed Pending Key column

ACTIVITY TYPE Date Time Activity ID	Object Host / Instance / DML Object OSUser as *DBUser* DML Column Name:	DML Old Value	Application on *Application Host* DML New Value
	DDL Object, ... DDL SQL		
UPDATE 2005-02-03 11:04:52 2	HERMAN-E / HERMAN-E / FinancialDemoDB.dbo.Commission eric.herman as *LUMIGENT-HQ\eric.herman*		SQL Query Analyzer on *HERMAN-E*
	TransactionID:	1124	
	CommissionAmtPurchased:	10	100000
UPDATE 2005-02-03 11:06:27 1	HERMAN-E / HERMAN-E / FinancialDemoDB.dbo.Claims eric.herman as *LUMIGENT-HQ\eric.herman*		SQL Query Analyzer on *HERMAN-E*
	CustomerID:	3	
	DateSubmitted:	2004-12-05 10:55:36.583	2005-02-02 10:00:36.000
	PendingClaimAmt:	250000	400000

LUMIGENT

Bottom Line - Need to Audit Data

- The DBMS underlying the organization's critical applications holds the crown jewels
- Security to prevent external unauthorized access is insufficient—internal threats to data assets are much more prevalent than external threats
- ***Any*** unmonitored access puts ***all*** data integrity at risk
- Regulatory compliance
  - Management must be able to rely on integrity of data to make regular certifications and assertions
- Best practice
  - Compliance (staying out of trouble) is the minimum effort — data auditing must be an integral IT practice to protect important corporate data assets