Deloitte & Touche

Auditing Application Systems

Maria Shaw

22 September 2003

Controls Framework (COBIT Definition)

Quality Requirements

- Quality
- Cost
- Delivery

Fiduciary Requirements (COSO Report)

- Effectiveness and Efficiency of operations
- Reliability of Information
- Compliance with laws and regulations

Security Requirements

- Confidentiality
- Integrity
- Availability

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- **Confidentiality**
- **Integrity**
- **Availability**
- Compliance
- Reliability of Information

IT Resources (COBIT Definition)

- DATA are objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.
- **APPLICATION SYSTEMS** are understood to be the sum of manual and programmed procedures.
- TECHNOLOGY covers hardware, operating systems, database management systems, networking, multimedia, etc.
- FACILITIES are all the resources to house and support information systems.
- PEOPLE include staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

Auditing Application Systems Approach

- Understand the business process or function that the application supports
  - e.g. Sales commission, order processing
- Meet with the business personnel to understand the business process
  - Map out the process
  - Identify application inputs, outputs, interfaces
  - Identify application controls and manual controls
  - Identify application outputs
  - Highlight any issues or concerns from the business owners

Auditing Application System Approach

- Review application system documentation
- Analyze the flow of transactions through the system
- Prepare a risk assessment to analyze the application's controls

Application Input Controls

- Authorization of end users
- Unique user ids and passwords
- Segregation of duties enforced by the application
- Audit trails turned on and reviewed periodically
- Review of system admin privileges
- Input authorization

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- **Confidentiality**
- Integrity
- Availability
- Compliance
- Reliability of Information

Application Input Controls

- Input data validation checks
  - Limit test – a test of reasonableness
  - Validity test – a comparison against master files
  - Self checking number – a check for accuracy
- Batch integrity of online or database systems
- Input controls for batch processing
  - Item count – to assure all items are processed
  - Control total – to assure a critical field of data is entered correctly
  - Hash total – may be a total of all order numbers
- Error reporting and handling

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- Confidentiality
- **Integrity**
- Availability
- Compliance
- Reliability of Information

Application Processing Controls

- Online systems – test the validation checks are applied to data being input
- Batch processing
  - Use of computer file identification systems (headers) to prevent use of improper data and program files (only payroll systems will process data labeled as payroll data)
  - Comparison of control totals gathered during input with total transactions processed.
- Processing Controls
  - Editing
  - Run-to-run totals
  - Programmed controls
- Review exception or error processing reports

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- Confidentiality
- **Integrity**
- Availability
- Compliance
- Reliability of Information

Application Output Controls

- Logging and storage of negotiable, sensitive and critical forms in a secure place
- Report distribution
- Balancing and reconciling
- Output error handling
- Output report retention
- Verification of receipt of reports

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- Confidentiality
- **Integrity**
- Availability
- Compliance
- Reliability of Information

Application Controls

- Purchased Application System
  - Stability of the software company
  - Support for the application software
  - Documentation
- Developed Application System
  - Application documentation (– program flowcharts, decision tables, data element definitions etc.,)
  - Application operations documentation (- input and output descriptions job restart/recovery, error messages etc.,)
  - End User documentation
  - Application support personnel

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- **Availability**
- Compliance
- Reliability of Information

Application Controls

- Backup and Recovery
- Application backed up periodically
- Tapes offsite
- Recovery procedures documented and tested

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- **Availability**
- Compliance
- Reliability of Information

Verify Application Controls

- Application controls include methods for ensuring that:
  - Only complete, accurate and valid data are entered and updated in a computer system
  - Processing accomplishes the correct task
  - Processing results meet expectations
  - Data are maintained

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- **Confidentiality**
- **Integrity**
- **Availability**
- Compliance
- Reliability of Information

Verify Application Controls

- Observe and Test Users Performing Procedures:
  - Review and test access authorizations and capabilities
  - Separation of duties
  - Authorization of input
  - Balancing
  - Error control and correction
  - Distribution of reports
  - Manual controls
  - Recovery procedures

COBIT
INFORMATION CRITERIA

- Effectiveness
- Efficiency
- **Confidentiality**
- **Integrity**
- **Availability**
- Compliance
- Reliability of Information

Application Controls

- Confidentiality
- Integrity
- Availability

Example Report

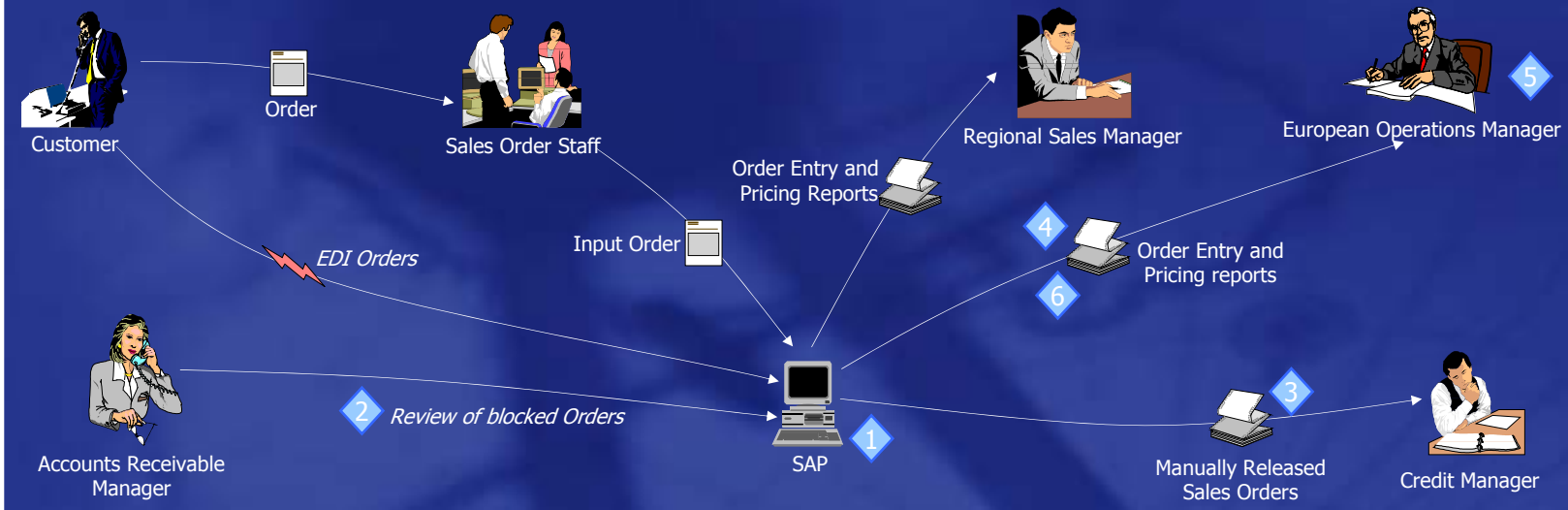
Revenue

Managing & Processing Orders

Invoicing, Sales Returns & Adjustments

Processing Cash Receipts

Maintaining Customer Master File



Key Controls

1. SAP performs certain validations before orders are processed further. For example, customer reference details are checked against Customer Master file records, system ensures completeness of order details and checks stock availability. Validation failures result in orders being placed in incomplete order queues which is checked daily by sales office staff.

2. All orders are automatically credit checked by SAP against agreed credit limits before they are processed further. Blocked orders appear on the blocked sales distribution listing which is reviewed throughout the day by the Accounts Receivable Manager.

3. Blocked orders that are manually released are reviewed daily by the Credit Manager.

Key Controls

4. Order reports are reviewed daily by Regional Sales Managers (CPD) and European Operations Manager (BSD) for unusual order quantities + prices.

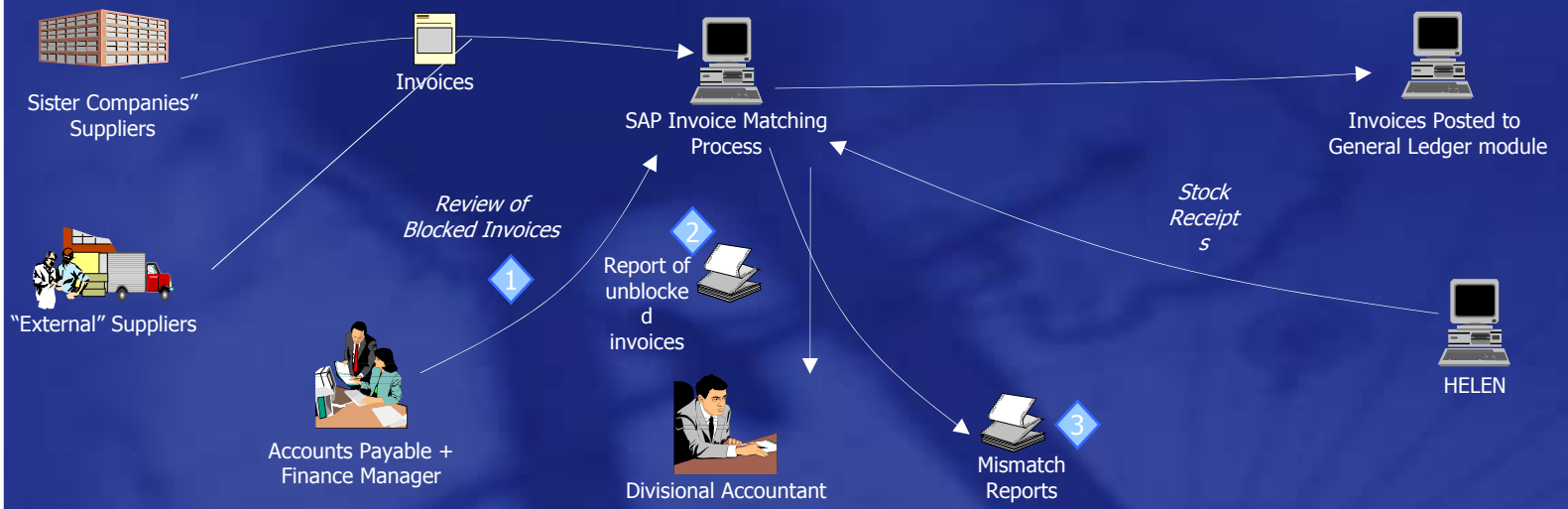
5. Some customers orders are processed through EDI. Sequential number checks are performed to ensure all orders are captured with error messages sent to the European Operations Manager.

6. Order pricing reports detailing prices < cost are sent to the Regional Sales Manager and European Operations Manager on a regular basis.

Example Report

Expenditure

- Purchasing
- Processing Accounts Payable
- Processing Disbursements
- Maintaining Supplier Master File



Key Controls

1. *All Suppliers* - Invoice price details are matched to standard costs on purchase orders. Any difference (zero tolerance) will cause the invoice to be blocked. Blocked invoices are reviewed by Accounts Payable and the Finance Manager on a daily basis.

   External Suppliers Only - Invoices are blocked for payment where there are quantity mismatches between supplier invoices and goods physically received and recorded on SAP (zero tolerance).

2. Divisional Accountants review month-end reports identifying all blocked invoices that have since been cleared.

Key Controls

3. Although they do not result in the blocking of invoices, the SAP system reports mismatches between the following which are investigated and actioned:

   •invoice and purchase order quantities - all suppliers;

   •invoice, supplier shipping notification and GRN quantities - Sister companies only.

Questions