

MIS 5121: Business Processes, ERP Systems & Controls

Week 10: *Data Interfaces*



Key Information Technology Risks

- System Security
- Information Security Administration
- Data Migration
- **Data Interface**
- Instance Profile Security
- Change Management
- Transport Security
- Table Security
- Data Dictionary, Program and Development Security
- Logs and Traces
- Firefighter access
- Powerful User ID's and Profiles
- Background Processing (Batch vs. foreground: real-time)





Data Interfaces: Control Concerns

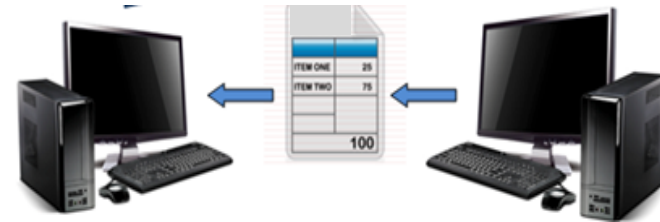


Data Interfaces



Data Interfaces: exchange data from one system to another

Goal: accuracy, completeness and timeliness of data - esp. those that impact financial results



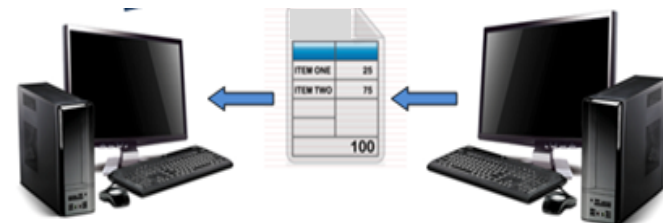
Data Interfaces: Process



Timing / Scope

- Event Driven (e.g. transaction)
- Scheduled / periodic
- Initiation (Start of process sequence)

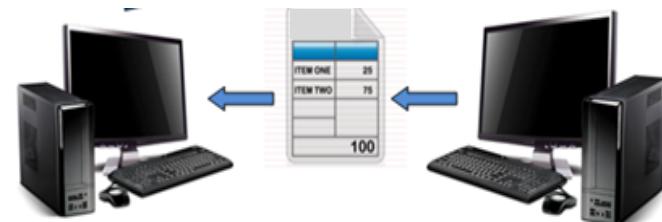
Systems could be internal or External



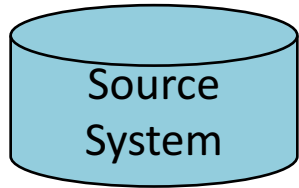
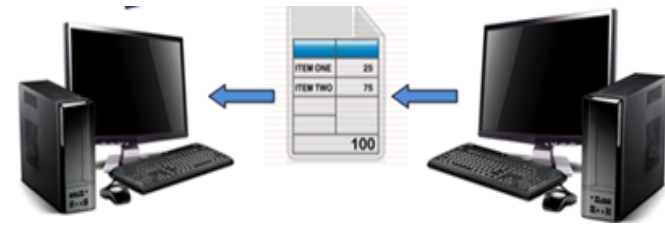
Data Interfaces: Process



- Extract from source system
- Transmit data to destination / target system
- Receipt of interfaced data by target system
- Verify received data is correct (e.g. right format), valid and complete
- Staging data prior to upload to target system
- Import into target system
- Validate data once imported



Data Interfaces: Risks



Data Interface



- Inaccurate or incomplete data extracted or pass over interface
- Duplicate data is extracted
- Data not extracted or passed timely
- Exceptions and errors are not detected or acted on to resolve
- Data not extracted in appropriate sequence
- Inbound interfaces with errors cannot be backed out
- Sensitive data not protected during transmission
- Data modified before, during, after transmission

Data Interfaces: Control Focus



- Adequate detection and prevention of duplicate data Processed
 - Some data (e.g. master data) just updated with latest value extracted (e.g. by Key match)
 - Transaction & Event data requires more duplicate controls
- Data sequencing and timing are monitored. Failures are reviewed, root cause identified and corrective actions put in place
- 'System of Record' clearly defined and process / application respects this
- Exceptions and errors are detected and procedure / method to review and resolve exists
- Sensitive data is sent via encrypted or secure channels only
- Adequate security and controls exists in source and target systems to prevent unauthorized modifications to data.

Data Interfaces Overview

Data Interfaces (usually on-going)

- Risks (Few)
- Controls (Few)

