



Application Review

November 2008





Content

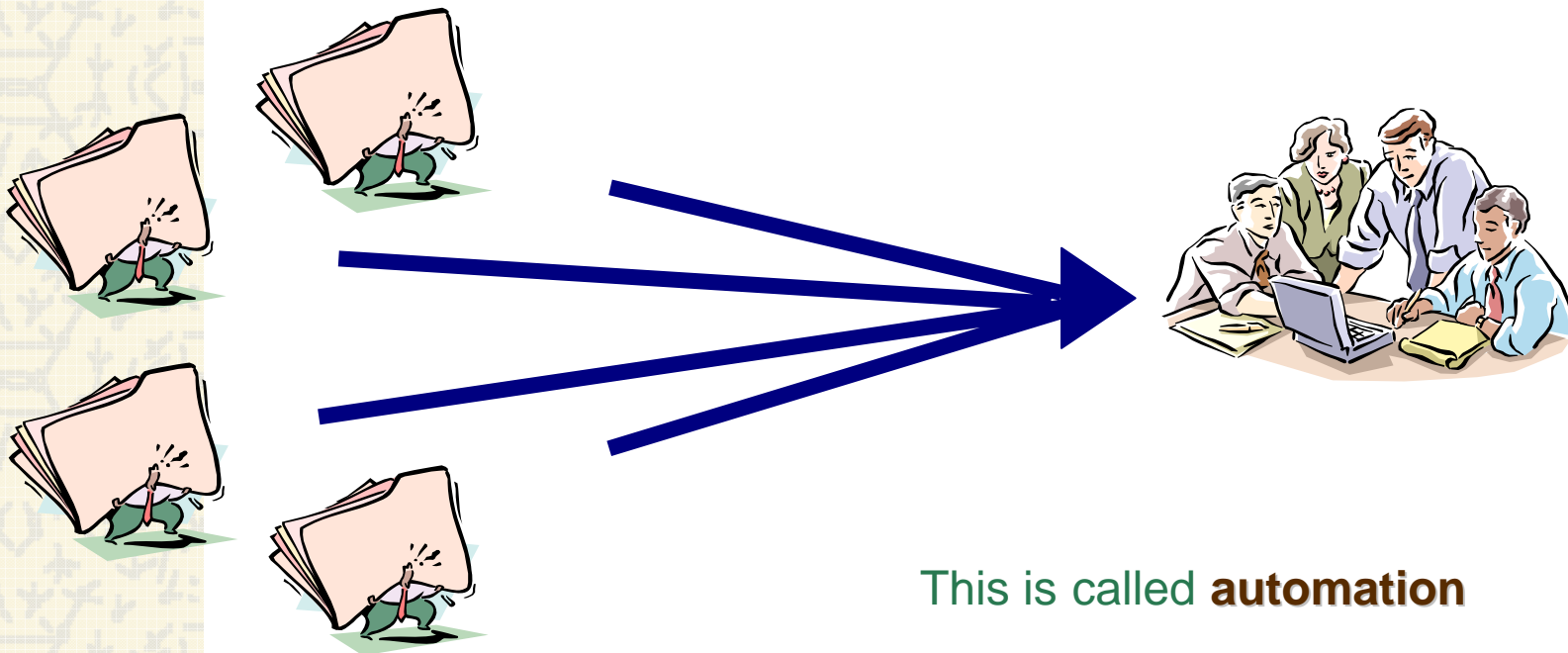
- What is an **application**?
- The **application** supports the **business process**
- **Significance** of an **application** within a business
- Changes in the **risk environment**
- Changes in the **control environment**
- Why **review** the **application**?
- Who is **responsible** for the **application functionality**?
- **Documenting** the **process** supported by the application?
- How to perform an **applications review**?
- Secrets of **success**



What is an application?

Back to the basics.....

An application is a machine that has been told through a program how to perform a process.



This is called **automation**



What is an application?.....

Can a simple process be automated?

Let's analyze a simple and common business process:

Elaborate receipts for purchase orders
placed by customers



The application supports the business process

What is needed to manually elaborate one receipt?

1. For each receipt it is needed: the item code, price, city and quantity ordered.
2. Locate the product code and identify the **price** (eg. \$100.00) 100.00
3. Write the **quantity** of items desired. (eg. 5) 5
4. Calculate and write down **amount due**: prices times quantity (5*100) 500.00
5. Calculate and write the **subtotal amount**: sum up all the amounts due 500.00
6. Identify the **tax percentage** based on the city (eg. 8.25%) 8.25%
7. Calculate and write down **tax amount** 41.25
8. Calculate and write down the **total amount**: subtotal plus tax amounts 541.25



The application supports the business process

How does the process go from manual to automated?

After doing a number of receipts, someone may notice that

- For each receipt the **same steps** are performed in the **same order**
- For each receipt the **same calculations** are made
- Each calculation results in **new data** that should be **written down**
- Data obtained or calculated is the **basis** for subsequent steps
- To validate that everything is correct.....
the same amount of time is invested twice for each receipt.

Maybe this simple process could be **automated**





Significance of an application within a business?

A simple application to execute the process of the example...
[Example receipt.xls](#)

What is the benefit of this automation?

- **Less data** to write down: code, quantity and city
- **Less time** to prepare a receipt
- **No need to review** each calculation and data for each receipt
- The **risk** of miscalculation for each receipt was **reduced**



Changes in the risk environment

Why change the manual process for an automated one?

- The likelihood of **mistakes** in the manual process is high
- Manual elaboration of receipts is **time consuming** and **inefficient**
- Several **pieces** of **data** are obtained, calculated and re-used for new calculations
- **Manual re-validation** of each receipt should be done to identify mistaken receipts
- Mistaken receipts would need to be **cancelled and redone**generating **unnecessary expenses** and **time**
- Entries in the **general ledger** would have to be **corrected**
- The business could **lose customers** and be subject to **criticism** by regulators





Changes in the risk environment

The risk to the process has changed

- **Incorrect calculations** programmed in the spreadsheet
- In case of program error, all receipts will **systematically** have the same mistake
- Accidental **changes** to the spreadsheet going **undetected**
- **Inaccurate base information** such as taxes by city
- **Conflicts** while using the application



Changes in the control environment

What is needed to mitigate the risk to the manual process?

- **Updated lists** of codes, prices and taxes are to be distributed
- All participants should have the **same lists** to work with
- **Calculators** should be provided and secured
- Receipts should be **revalidated** (data and calculations) **at least once**
- Receipts should be **re-produced** by a supervisor
- Copies of receipts should be **filed** and **protected**
- Entries should be **manually** entered in the **general ledger**

Changes in the control environment

What is needed to mitigate the risk to the automated process?

- **Calculations** programmed in the spreadsheet should be reviewed
- **Changes to the spreadsheet** should be controlled
- **Base information** should be entered and centrally maintained
- **Access to the application** and the information should be managed
- **Concurrent** access to the application should be arranged
- **Periodical validation** that the application continues to work as planned
- Review of a **limited number** of receipts or a retrieval provides assurance
- One **interface** could up-load all entries into the general ledger



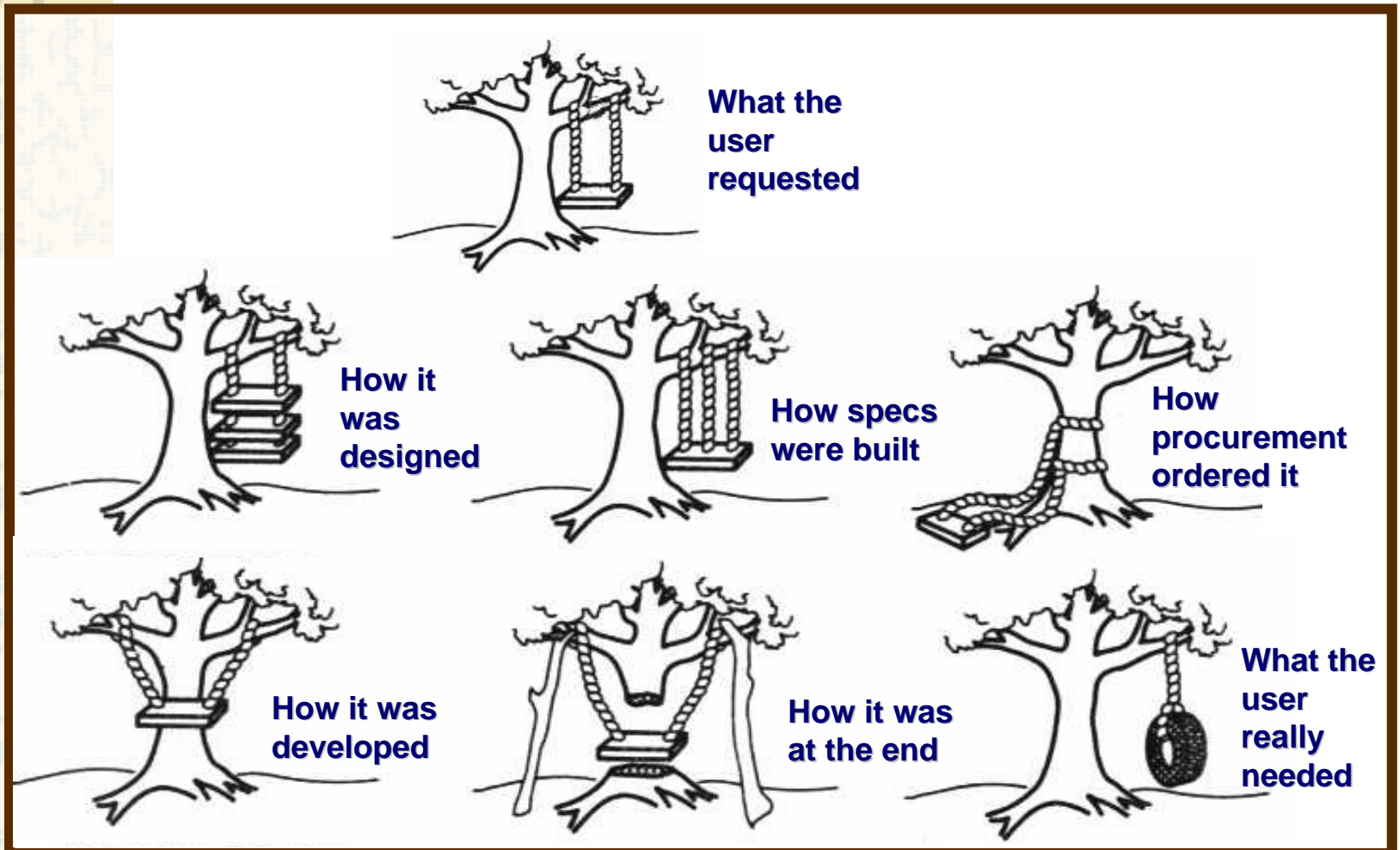
Why review the application?

The computer does itno need to review it?

- The application executes instructions programmed by a chain of human beings.....therefore it could be **mistaken**
- Human beings sometimes don't know what is needed...but they need to deliver.....therefore **requirements and product are not always accurate**
- If it were a manual process, validation should be done on a case by case basis.....because each receipt has the same **probability of human error**
- Since the receipts are produced by the application, validation is needed to ensure that the program's calculations and assumptions are **systematically correct**
- The application under review could be like the **following case**



Why review the application?



Why review the application?

The computer does the process.....no need to review it?

The Information Systems auditor should ensure that

- The application functionality **supports the business process**
- The **controls** to the risks of the process are properly **built into** the application functionality
- The application **functionality evolves** with the needs of the business process
- The application functionality is **protected from** unauthorized **changes**
- The **access to the information** contained in the application **is managed**





Who is responsible for the application functionality?

Who is ultimately responsible for the application?

- The **owner** of the information and the business process

Who is the owner?

- Whoever obtains the **business benefit** out of it

Let's think of another simple example:

If someone wants to build a closet for a bedroom.....

Who has the ultimate saying on how the closet should be, how much should be spent and what materials to use?

The carpenter OR the owner of the bedroom??????



How to document the process?

Identify the steps and flow of the business process:

- Variable **input data**
- **Calculations**
- Sequential **steps**
- Milestones, **risks and controls** (including requirements such as SOX)
- Steps that require independent **validation / approval**
- **Interaction** with other business processes / applications
- Portions of the process done **manually** and executed by **an application**
- **Accountability** for every part of the process
- **Example receipt.xls**





Why document the processes supported by the application

Documented process is the framework to determine if:

- The application functionality **fulfills** the **business needs**
- The **milestones** of the business process are **embedded** in the functionality
- Applicable industry **standards** and **regulations** are **built in** the application
- **Responsibility** when parts of the process performed by third parties
- The inherent **risks** of the automated process are automatically **controlled** by the application or require human intervention when certain milestones are reached



Why document the processes supported by the application

Before starting the application development:

- The **business process** should be **clearly documented**....Written in English to be translated into machine language
- Have a clear “**what are we automating?**”.....Otherwise, the result is the **automation** of the **disorganization**
- Have a clear “**how should the process be executed?**”.....Otherwise, the automated process will render **questionable results**
- Have a clear “**what regulatory requirements are needed?**”.....Otherwise, **compliance** with regulations like **SOX** would be **compromised**
- The business owner should be involved as much as technology areas.....



How to review the application?

The Information Systems Auditor should:

- Understand the **business process**
- Know the **company's strategy**
- Identify applicable **standards** and **trends** of the industry
- Determine applicable **regulations**
- Have a close communication with the **product reviewers**



How to review the application?

Some aspects that could be reviewed are:

- Architecture
- Functionality
- Software administration and Licencing
- Compliance with applicable regulations and standards
- Vendor Management
- WEB management
- Resource Management
- Information Security
- Problem Management
- COB

Note: Depending on the size of the organization and the audit function, the potential scope for information systems review may be covered by one or multiple groups. The IS auditor should adhere to the applicable policy



How to review the application?

Some more technical aspects:

- Hardware Administration
- Hardware configuration
- Networks
- WAN
- Privileged accounts
- Database management
- Development Process

Note: Depending on the size of the organization and the audit function, the potential scope for information systems review may be covered by one or multiple groups. The IS auditor should adhere to the applicable policy bbb



Secrets of success

The Information Systems Auditor may consider

- If a business process has **automated controls**.....**application review** is needed
- The IT auditor should **understand the business process** to be able to assess the **application functionality**
- The IT auditor should gain **understanding of the application itself**
- The IT auditor should know in advance the **risk level of the applications**
- The IS auditor should understand the **type of information** in the application under review
- The Information Systems Auditor should be part of the **planning process**
- The more **retrievals** the better the application can be reviewed



Secrets of success

The Business Auditor leading a review that requires application review may consider:

- The Responsible for the Review team should **understand the significance of the applications** within the business under review
- The Responsible for the Review should **determine in advance the IT resources needed** to review the number of applications and the risk level
- The Responsible for the Review and the IS auditor should determine the **scope of the application review** and build the planning documentation detailing planned omissions
- Insufficient IT resources result in **poor application review**
- A comprehensive list of **deliverables** for the application review **should be requested in advance**, some of them take time to be produced





Questions?

