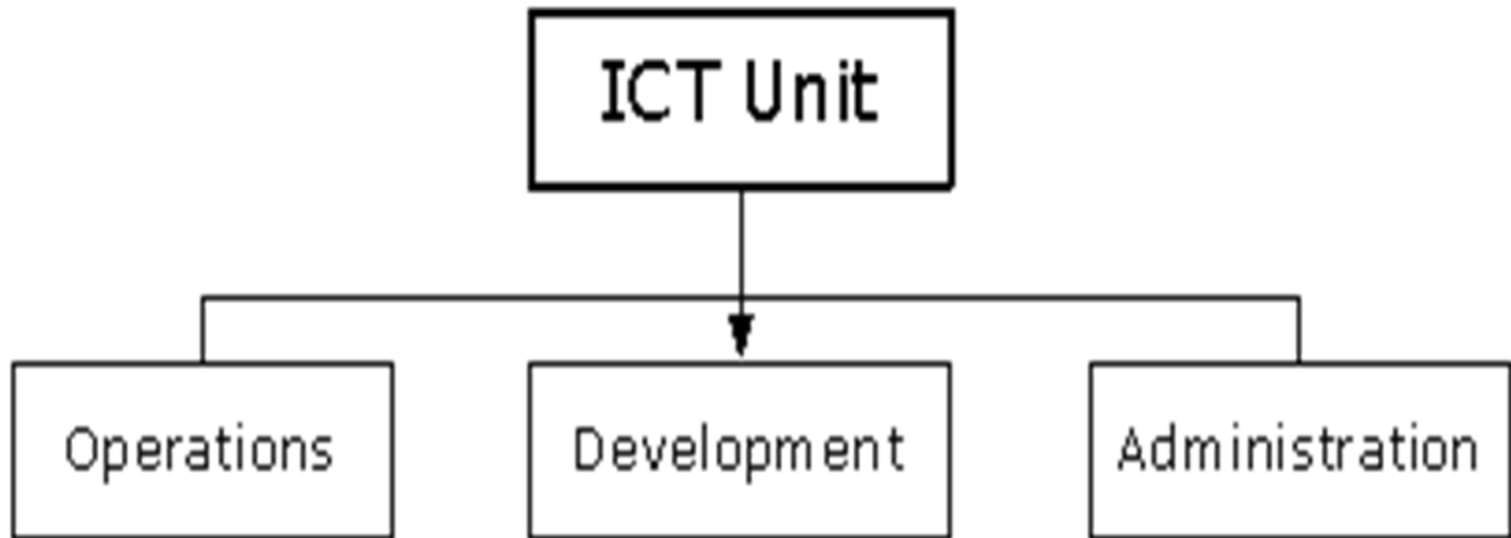



Challenges facing staff in an eBusiness workplace

Auhor Aronovici Gabriela
MySoft SRL

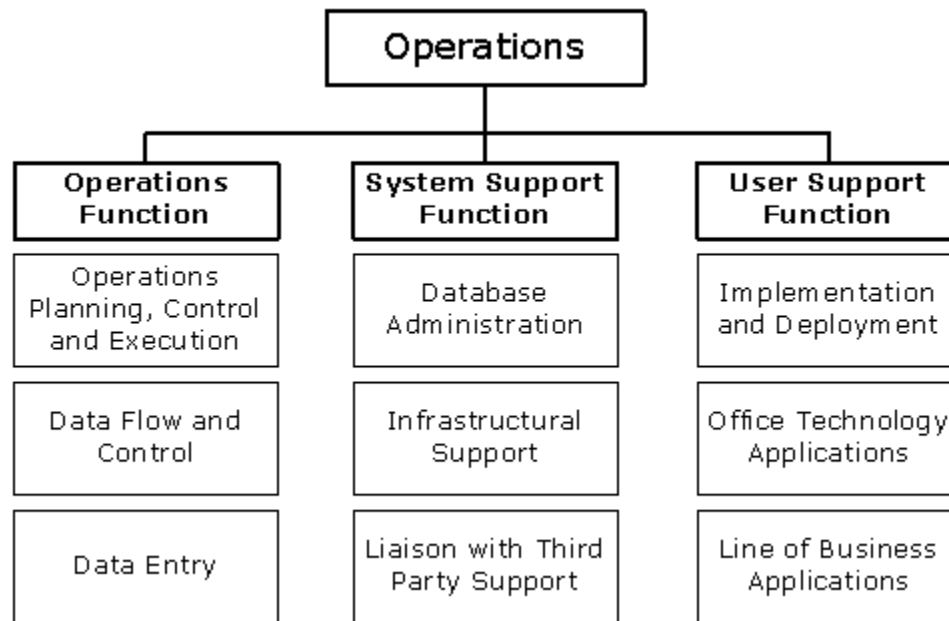
An Organization Chart for a generic ICT Department in an eBusiness workplace



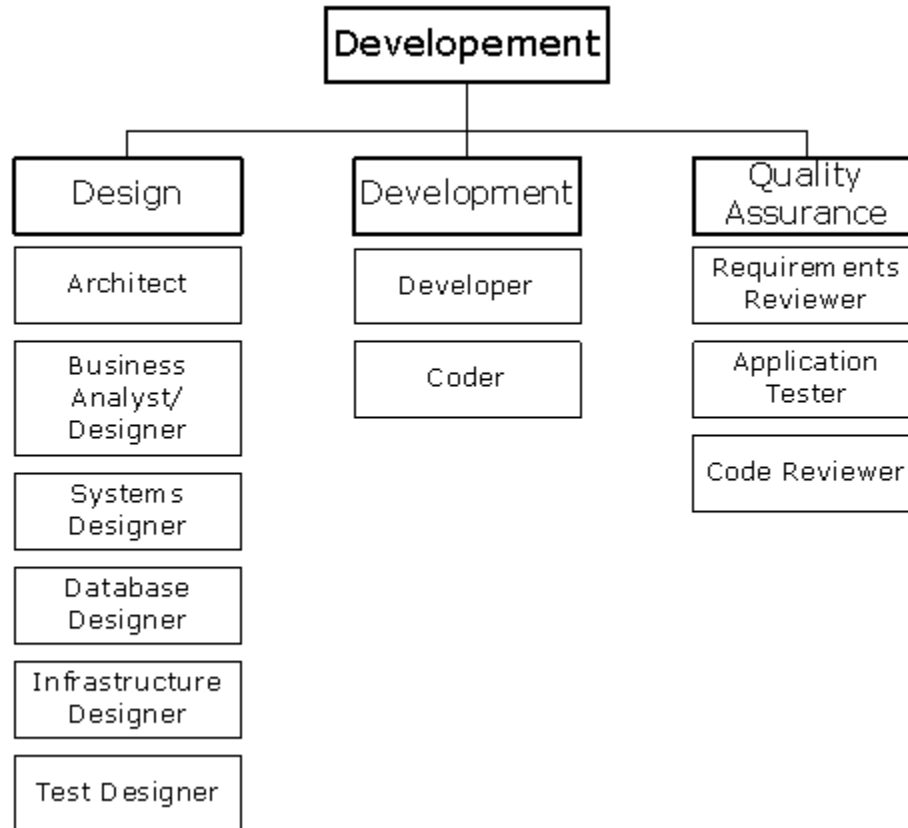
Managing ICT Human Resources

- Organize the Structure of the ICT Unit
 - Identify the Required Competencies per Position
 - Identify Actual Competency Levels of all Staff
 - Analyze Competencies to Identify Training Requirements
 - Identify Training Resources
 - Manage Training Material
 - Maintain Training Records
 - Define Recruitment Standards
- 

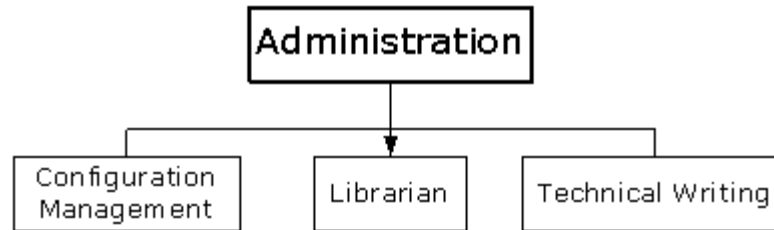
Operations



Development



Administration



Configuration Management

- To ensure that the initial Configuration is properly setup
- To ensure that the workflow for the Change Requests is being followed and properly documented
- To ensure that all changes are properly reflected within the database
- To prepare and disseminate the various analyses, reports and results of Configuration Analysis.

Librarian


The Librarian works closely with the Configuration Management person. The main responsibility of the Librarian is to physically control a variety of items in the ICT Unit such as backup media, supplies, documentation of all types (System, training, data sheets, systems designs, etc), training material (Documents, videos, CDs, etc), software products, Etc.

Technical Writing

Often referred to as Content Development, Technical Writing is often required in an ICT Unit for the development of such documentation as Help Files, User Procedures, Standard Operating Procedures, Instructions and Guidelines, Etc.

Identify Functions to be Secured

Typical functions are:

- ▶ Access to the network
 - ▶ Access to a specific PC desktop
 - ▶ Access to a particular database application
 - ▶ Access to specific web sites
- 

Assign Privileges and Access Rights

Standard Operating Procedure:

- 1) The Department's management must decide who can assign such privileges to the various members of staff.
- 2) Ensure that the previous Activity of identifying all Privileges and Access Rights has been completed.
- 4) Prepare a list of all staff that might be able to access the system.
- 5) Group the staff by groups to ease the task of assigning privileges. For example, all secretaries will have the same set of privileges. A new secretary will automatically inherit the same privileges as the rest of the group.
- 4) The above two lists will form a matrix or a spreadsheet. At the top of each column, enter the type of access. In each row, enter the name of the staff.

For example, under the column **Exchange Rates** and across from the **Chief Accountant** row, you can enter **ALL** to signify that this person can create, read or retrieve, update or delete a currency record. On the other hand, a specific person, such as the Store Keeper, will have only R under his name because he can only Retrieve the exchange rate but not delete it, update it or create a new currency code.

Protection Against Viruses

- 1) **Backup:** one of the best insurance schemes against infection is proper data backup. This includes all operating or application software. Review the earlier activities in this Section for a discussion of backup procedures.
- 2) **Use up to date anti-virus products** with the latest patches and upgrades. These have to be licensed to run on the various machines in the center.
- 3) **Use up to date virus definitions:** ensure that a responsible person regular checks and updates the data definitions of the viruses. Many centers wrongly assume that if they have the latest version of the software, they are protected. It is estimated that 200 new viruses are identified per month. Developers of anti-virus products frequently release new virus definitions to meet this surge.
- 4) **System scans:** on a regular basis, scan the whole system including zipped files. This can be carried out at night when there is no work load on the system.
- 5) **Importing data into the site:** in the sites where there is a lot of traffic of data to and from the outside world, it may be required to implement strict techniques about using data on floppies or CDs or zip drive disks coming from the outside. Some centers disable all such units. Others remove them completely. In the case where a center cannot remove a CD drive because of its internal use, it becomes critical to discipline users to scan CDs for viruses before using them.

Backing Up

- ▶ **Objectives:** to prepare a Backup procedure observing all backup requirements stated in the Backup Definition List and to ensure that there is a record of all backups taken for all types of information. This is the most crucial Activity to be carried out by the Department and it aims at maintaining Information in total integrity. It may be time consuming and it may be costly, but it is an insurance against data loss or corruption.
- ▶ **Risks:** not backing up the data on a regular basis will cause the Department to be exposed to loss of data and software items.

How ?

- ▶ **Centralization of the Backup Register:** in the case where Departments have several sites, servers, applications, Etc., it would be necessary to have a centralized register. Copies of printed forms can be sent to such a location. If the register is setup on a minor database, then it can either be located centrally and made accessible to all operators or different databases can be consolidated on a regular basis.
- ▶ **Configuration Management:** it may be suitable to setup the Backup Register as part of the Configuration Management database.
- ▶ **Securing Backup:** some centers follow the recommended practice of carrying out the backup by well trained personnel. In order to do that, some security measures may be implemented so that only such persons can carry out the backup.

Disaster Recovery Procedures

Standard Operating Procedure

- ❖ Prepare the following documentation before the Disaster:

Emergency Procedures: describes the immediate action to be taken following a major incident which jeopardizes business operations. Such actions are usually not ICT related and would cover such activities as: moving files or special equipment, ensuring personnel get to the new location, moving support to the new location, informing external users such as citizens or companies of the change, Etc.

Responsible: specify the individuals responsible for executing each component of the plan.

Configuration: prepare a document that describes the configuration of the recovery system to avoid reconfiguring such elements as user names, passwords, directory structure, service packs, Etc.


- ❖ **The Recovery Procedure:** a document that describes the Recovery Procedure in a step by step fashion.
- ❖ **The Recovery Test Plan:** a document that shows the procedure needed to certify that the Recovery has been properly executed. For example, the Test Plan can include: File counts, File sizes, Database record counts, Date checking
- ❖ **Backup Media:** prepare an offsite location for the backup media. It is recommended that the media be stored at a significant distance from both the Production and the Recovery environment in order to avoid total loss in the event of a widespread disaster. It is vital that the backed up media can be accessed in a hurry, so again, it is best to have recourse to multiple backups in different sites.

Using and Supporting Office Technology Products

- 1) **User Training:** The first step to ensure proper use of Office Technology Products is to provide regular training of users.
- 2) **Encouraging use of office technology products:** most users will be happy using 10% of a word processor and a spreadsheet. It does not require much more effort to improve the competence in such products.
- 3) **Standardized Directory Structures:** most users have a tendency to create documents all over the disk on their PCs. This usually results in document losses, duplication and difficulties while backing up. It is recommended that the Department establish a standardized directory or folder structure that can be used by all users. This has the added benefit of allowing easier support and backup.
- 4) **Standardized File Naming:** for files that are used internally and between different users, it is best that a standardized naming procedure is followed.
- 5) **Backup procedures**
- 6) **Using standard forms:** many organizations fall into the trap of using different forms for their standard correspondence. Forms can be standardized and setup as templates on the user systems or on the central server.
- 7) **Version Issues:** It is therefore important to ensure that all users have the same versions of office technology products or at least have the proper converters for such products.
- 8) **Information Sharing:** Such information as the following should be shared: telephone lists, email addresses, schedule of events, project lists, supplier names and records, file structure, reference register, document registers, types of templates, placed orders, Etc.

User Support

The support is for all types of applications and requirements:

- ✓ **Hardware:** its fault reporting, usage, preventive maintenance and installation
 - ✓ **Office Technology Applications:** usage, installation, upgrades, updates, configuration and error reporting.
 - ✓ **Telecommunications:** connections, installation, configuration fault reporting.
 - ✓ **Running specific applications of the Department.**
- 

What this Presentation Hopes to Achieve

- ▶ To provide the Management of a Department with reasonable assurance that business objectives will be achieved through the ICT Systems, Resources and Processes and that undesirable events will be prevented or detected and corrected.
- 