Equipments:

1. Virtual PCs: **8** for the **Marketing** department, **3** for the **HR** department, **10** for the **Web Developers** department, **24** for the **Sales** department, **2** for the **IT** department, **4** for the **Management** department.
2. Router
3. 5 Switches
4. 4 Printers
5. Old server, new server, print server
6. Firewalls
7. Ethernet cables

Architecture:

OLD BUILDING:
In this building, we set up three VLANs:

1. VLAN10 for the Sales Department with an ip address of 192.168.0.10, 24 vpcs were connected together to a switch.
2. VLAN30 and VLAN40: due to the small numbers of vpcs in each department (2 for IT and 4 for Management), we decided to put them on one network connected to a switch with different IP addresses since they are two VLANS and completely different from each other (192.168.2.10 and 192.168.3.10 respectively).

NEW BUILDING:
There are also 3 VLANs:

1. VLAN20 for the Marketing Department with ip address of 192.168.1.10
2. VLAN50 and VLAN60: due to the small numbers of vpcs in this building too, in each department (3 for HR and 10 for Web Developers), we decided to put them on one network connected to a switch with different IP addresses since they are two VLANS and completely different from each other (192.168.4.10 and 192.168.5.10 respectively).

Now, each VLAN is connected to the old server in the building, and between each switch and the old server there is a firewall which provides protection against outside cyber attackers by shielding the network from malicious or unnecessary network traffic.

As we know, each company uses printers in their daily work days for many purposes. That's why we've added a print server connected to 4 printers in order to manage print requests and make printer queue status information available to end users and

network administrators. This method helps us handle complex environments and of course it’s easier for end users and is more secure.

Back to the servers, they’re connected to a router which will help the 2 buildings communicate with each other, also the VLANS in the same building.

Finally the router is connected to the internet through the firewall. A firewall is needed in this case specifically because we are connected to the WAN and public networks can be insecure as well.