Assets, Vulnerabilities, Threats

Assets	Vulnerabilities	Threats
Office Rooms	Lack of access controls.	Unauthorized entry into facilities, rooms or offices.
	Use of old equipment.	Theft, vandalism, or sabotage.
	Lack of maintenance.	Maintenance errors.
Cabinets	Lack of maintenance.	Maintenance errors.
	Inadequate capacity.	Industrial accident.
Desktop Computers	Use of old IT equipment.	Equipment failure.
	Inadequate change control.	Maintenance errors.
	Downloads from internet not controlled.	Increased chance of viruses.
Servers	Use of old IT equipment.	Equipment failure.
	Inadequate change control.	Maintenance errors.
	Test and operational environment not separated.	Increased chance of unwanted downtime if rebooting an operational server instead of test.
	Sensitivity of equipment to temperature changes.	Equipment failure.
Wireless LAN	Poor internal audit of equipment.	“Ghost” devices could be used to bypass corporate controls.
	Inadequate IT cabling.	Interruption of communication services.
	Over dependance on one device.	Equipment failure.
Printers	Use of old equipment.	Equipment failure.
	Wrong configuration of network access.	Unintentional access to network.
	Over dependence on one device.	Equipment failure.
Mobile devices (laptops, smartphones)	Use of old IT equipment.	Equipment failure.
	Inadequate change control.	Maintenance errors.
	Downloads from internet not controlled.	Increased chance of viruses.
Third Party Data	Poor selection of test data.	Unintentional disclosure of data / information
	Inadequate change control of documents and data	Breakdown of communication links.
	Confidentiality level not clearly defined	Improper use of IT systems or information.