Module Details		Trainee's Details	
CRYPTOGRAPHY AND NETWORK SECURITY			
LEARNING OUTCOME ……..			
Sector	TECHNICAL SERVICES	**Roll No**	…….. …….. …….. …….. …….. …….. …….. ……..
Sub-Sector	ELECTRONICS AND TELECOMMUNICATION TECHNOLOGY	**Class**	**Y4 / B-TECH / ETT**
		FORMATIVE ASSESSMENT 1 / G7	
		Trainer's Details	
Certificate	Bachelor of Technology in Electronics and Telecommunication	**Name**	E.NTIRENGANYA

1. Learning Objectives

By completing this case study, students will be able to:

1. Understand what virtualization means and how it can be used in telecommunication companies.
2. Identify the types of virtualization: server, storage, and network.
3. Recognize the main security risks when using virtualization.
4. Suggest disaster recovery and incident response strategies in a virtualized setup.
5. Relate classroom knowledge to real-world challenges faced by companies using virtualization.

2. Case Description

Independent professionals working in DevOps, together with companies such as WE-MEP Consultant Ltd, often support small and medium businesses that need reliable IT systems but cannot afford expensive hardware. By adopting virtualization technologies, they can help these businesses run services on virtual machines (VMs) or containers instead of using many physical servers. This makes the system more cost-effective, easier to expand, and quicker to manage.
However, this change also brings **security challenges**. Virtualization can create new risks such as **attacks on the hypervisor, too many unmanaged VMs (VM sprawl), and risks of data leakage** because resources are shared.

3. Virtualization in Telecom and IT Services

- **Server Virtualization:** Running many operating systems on one server using a hypervisor (examples: VMware ESXi, KVM).
- **Network Virtualization:** Using software to replace physical routers, firewalls, and load balancers. In telecoms, this is called **NFV (Network Functions Virtualization).**
- **Storage Virtualization:** Joining many storage devices into one logical unit so they can be used flexibly.

For companies like **GTT Ltd** or **Prisco**, this means running firewalls, VPNs, and even customer management systems as **Virtual Network Functions (VNFs)** or as **container-based services** instead of expensive hardware.

4. Security Concerns and Solutions

1. **Hypervisor Security** – Hackers may attack the hypervisor. *Solution:* keep it updated and apply strong security settings.
2. **VM Sprawl** – Too many unused or unmanaged VMs can increase risks. *Solution:* manage and monitor all VMs carefully.
3. **Shared Resources** – Different clients may share the same hardware, leading to possible data leaks. *Solution:* separate networks, use strong encryption.
4. **Insider Threats** – Staff may misuse access. *Solution:* apply strict access controls, role-based permissions, and use MFA (multi-factor authentication).

5. Disaster Recovery Plan

- **Backups:** Store VM snapshots both onsite and in the cloud.
- **Redundancy:** Run systems in more than one datacenter or server room.
- **Failover:** If one server fails, services continue automatically on another.
- **Testing:** Practice recovery plans regularly.

6. Incident Response Plan

1. **Detection:** Monitor system logs and virtualization tools for strange activity.
2. **Containment:** Quickly isolate the affected VM or network.
3. **Eradication:** Remove the threat and patch vulnerabilities.
4. **Recovery:** Restore services from a clean backup.
5. **Lessons Learned:** Review what happened and improve policies.

7. Case Discussion Questions

1. What benefits do companies like Freelancing in DevOps gain from virtualization?
2. What new risks are introduced compared to using only physical servers?
3. How can small companies secure their hypervisors against attacks?
4. Should they use VMs or containers for telecom/IT services, and why?
5. How can disaster recovery be improved with virtualization?

8. Conclusion

Virtualization helps companies like **WE-MEP Consultant Ltd**, **GTT Ltd**, and freelance DevOps teams provide modern IT services without large investments in hardware. It improves flexibility, reduces costs, and allows quick service delivery. But at the same time, it introduces new risks that must be managed. By setting up **security measures, disaster recovery strategies, and incident response plans**, these companies can enjoy the benefits of virtualization while keeping systems safe and reliable.