1. **IT Asset Management** – Keeping track of all the computers, software, and other technology a company owns to make sure they are working properly and being used efficiently.
2. **Vulnerability** – A weakness in a computer system or software that hackers or viruses could exploit to cause damage.
3. **Obsolescence** – When technology or software becomes outdated and no longer useful because newer versions are available.
4. **Compliance** – Following legal rules and industry standards to make sure a company's technology and data are secure and properly managed.
5. **Maintenance** – Regular check-ups and updates to keep software and hardware running smoothly.
6. **End of Life (EOL)** – When a company stops making or supporting a product, meaning it won't get updates or fixes anymore.
7. **End of Support (EOS)** – When a company stops providing customer service and security updates for a product.
8. **End of Maintenance (EOM)** – When a product no longer receives regular fixes or updates from the company.
9. **Asset Hygiene** – Keeping technology and software in good condition by regularly updating, securing, and removing outdated systems.
10. **Crown Jewel** – The most important and valuable assets in a company's IT system, like sensitive data or critical software.
11. **Inventory** – A list of all the IT assets (computers, software, servers, etc.) that a company owns.
12. **NVD (National Vulnerability Database)** – A government database that tracks security weaknesses in software and systems to help companies stay protected.
13. **Patch Management** – Patch Management is the process of regularly updating software, applications, and systems to fix security flaws, improve performance, and add new features.