|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Non repudiation | Accountability | Authenticity | reliability |
| Hardware |  | **In terms of a system, it refers to the destruction of a component from the system and the replacement with one that performs the same function, but not the original.** | **The most vulnerable parts of an organization are their hardware, which can be intentionally damaged or stolen.** | **hardware faults are mostly physical faults** |
| Software | **Software code is open source as well as everything else** | **Due to the fact that the program code is copied, future software issues cannot be corrected.** | **The software's failures cannot be held accountable by anyone.** | **Faults in software are design mistakes that are difficult to visualize, classify, detect, and correct** |
| Data | **Viruses and malicious files are not tested** | **The documents and files received are fabricated and are not genuine.** | **The program does not provide a mechanism for checking whether files are damaged, tampered with, or deleted.** | **The system should automatically generate backup copies of critical files to minimize the risk of data loss.** |
| Communication Lines | **Therefore, when a message is sent, the receiver can prove that the message was actually sent by the alleged sender.**  **In the same way, a sender can prove that the alleged receiver actually received a message.** | **Modification of a message means that some portion of it has been changed** | **messages are delayed or reordered, to produce an unauthorized effect.** | **Assessment of the reliability of transmitted messages over concatenated** |