**IT Assertions:**

|  |  |  |
| --- | --- | --- |
| **IT Assertions** | **Description** | **Control Examples** |
| Secure | IT systems are not accessible by non-authorized individuals, both inside and outside of the organization. This should include a combination of prevent, detect, and correct controls. | * Unique usernames * Passwords * Firewalls * Intrusion Detection Systems |
| Available | IT systems are ‘up’ and running when needed. | * Monitoring * Problem / Incident Response |
| Confidential | Data in IT systems is restricted to authorized individuals only. This is similar to Secure, above, but the focus is on data, not necessarily systems. | * Encryption |
| Integrity | IT systems perform their intended function correctly, completely, and timely. IT systems do not corrupt the data they process. | * Monitoring * Problem / Incident Response |
| Scalable | IT systems can be expanded (‘scaled’) to meet the volume of processing needed. | * Automated ‘spinning up’ of new virtual machines to meet peak volume, such as holiday shopping. * Capacity monitoring and response |
| Reliable | IT systems consistently perform their function complete, accurately, and timely. | * Change management (testing) |
| Effective | IT systems achieve their designed purpose. | * Any business-related control, such as a 3-way match between PO, receipt of goods, and invoicing. Then, the system kicks out a check. |
| Efficient | IT systems enable the organization to complete their tasks with greater quality, less expensively, or faster (‘better, cheaper, faster). | * Any control focused on ‘better, cheaper, faster.” |