1. Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)?P1

Factors:

People: The data, devices, personal information and facilities in which individuals for the organization in any capacity works is secured properly inventoried.

Information: The information relating the organization’s assets, facilities and critical information is properly secured and inventoried.

Technology: Information systems, physical devices, software platforms and applications within the organization are inventoried.

Facilities: Facilities that enable the organizations working environment is properly secured and inventoried

The assets that are critical in nature will play the most crucial role in terms of holding the key functionalities that the organization must have, and if they are on being at high risks, it will severely hit the reputation of the organization in very excruciating manner, so, assets do influence the inventory system.

1. Are both owners and custodians of assets documented in asset’s description?P2

People

Information

Technology

Facilities

The owner is held accountable for the data. As owner is considered to the part of the senior management or head of the establishment. Owner is responsible for laying out the data security classification. The custodian is concerned with what controls are, his duty is to implement them on behalf of the owner.Their roles clearly state that their priorities, which is imperative that their information should be documented in the asset description.

1. Are all the services which covers all the resources are prioritized from classification and their business values?

The services should cover all the prioritized resources, decisions on investments in IT are both critical and contentious. The reason behind this question is if a company’s strategic context, managers can identify business and IT maxims that can help them determine the IT infrastructure capabilities necessary to achieve business goals.

1. Is there any asset description update when some sort of change has been occurred within the asset?

IT assets are constantly moved, on rapid pace depreciate and require constant update and replacement, so in order to keep track of those updates, the update description should be added.

1. Is there any technique employed to discover what’s in the network or what services are offered by the network?

It is important to know what services are being offered by the network. Mapping the services would give the idea about the open and non-standard ports in the network. Discovering TCP/IP network services on system such as web or mail services is crucial since it would give the idea of ports that are running the said service.

1. Is there a standard set of tools or methods in use to identify and monitor vulnerabilities in assets?

After analyzing the potential services offered by the network, an authenticated vulnerability scan must be performed because it will give more accurate results since it will come down to data and information. It will give valuable insight and help prioritize the vulnerabilities that would compromise the system.

1. Is a repository used for recording information about vulnerabilities and their resolution?

Yes a repository is used, because organization owners and repository admins receive security alerts, the cyber team will detects a vulnerable dependency in an organization repository. GitHub regarded as a well reputed firm, because their services provides security alerts when a there is a diagnose of a vulnerability.

1. Have stakeholders for vulnerability management activities been identified and made aware of their roles?

The stakeholders have been well equipped for vulnerability managements, risk related to performance of a vulnerability will be reported to the relevant managers. The staff will be given frequent training sessions. They will get to know the basic knowledge of tools for sensing any vulnerability if it exists.