# **Scope**

## **In Scope**

Hardware – including PCs, laptops, tablets, servers, routers, switches, modems, wi-fi devices, printers, ethernet ports – basically anything which has a presence inside the network

Software – any installed software – including OS. This includes versions

Firmware – of any hardware with firmware – Version No

## **Out of Scope**

Phones – while they may present a risk, this may be considered too intrusive.

Suitability of existing hardware.

Penetration Testing

# **Risks**

1. Company unhappy to agree to terms of Assessment
2. Company is very busy – difficulty gaining access
3. Need co-operation of IT support to gain access to server
4. Company is currently for sale.
5. Investigation causes one or more services to fail (unlikely)
6. **Risk Matrix**(Kloppenborg, T et al, 2018 p371)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Insignificant | Minor | Moderate | Major | Catastrophic |
| Almost Certain  (>90%) | High | High | Extreme | Extreme | Extreme |
| Likely  (50-90%) | Moderate | High | High | Extreme | Extreme |
| Moderate  (10-50%) | Low | Moderate | High | Extreme | Extreme |
| Unlikely  (3-10%) | Low | Low | Moderate | High | Extreme |
| Rare  (<3%) | Low | Low | Moderate | High | High |