



STAY SECURE

Infrastructure Security Assessment

Compliance Audits don't focus on Security

Too many times companies performing Compliance Audits don't actually concentrate on the security level of the physical Network Infrastructure.

Compliance audits focus on Policies and Procedures, Documentation, Log Files, and Company Staff Training but only give a cursory glance at the infrastructure.

While these other factors are important parts of compliance, overlooking the Security State of the Physical Infrastructure is asking for security holes that will allow breaches.

Good Policies and Procedures, Documentation, and Staff Training are critical but your Network Infrastructure is your last line of defense when everything else fails so you need to know if your network will be your failsafe or your downfall..

Don't use Compliance Documentation to just create the appearance of compliance. An Infrastructure Security Assessment will test the **actual security** of your PCs, Servers, Firewalls, and Network.

- Test the current state of your server hardening and PC security.
- Find all the applications installed on your servers & PCs.
- Determine the patch level of all your Windows Operating Systems and each application.
- Test your Firewall's Security.
- Physical Security is a key part of your infrastructure security so it must be tested too.
- Detailed Audit Reports so you know the actual security state of your network and what problems need to be remediated.



240.686.2012 tel 240.686.2013 fax
Gaithersburg, Maryland
msconsulting.com