Security Audit

Identify a clear infrastructure security roadmap – quickly.

Is your infrastructure secure?

Despite the investments companies have made in technology, without a continuous detailed audit of its effectiveness and a proactive element to its management, it is unlikely to be 100 percent effective.

The true value of a secure infrastructure is only visible at the detailed level – it's not appropriate to expect a one-size-fits-all approach to work for every company.

More organisations are today tasked with the need to deliver governance and compliance, which includes the operation of IT systems and data security. These are, for many, critical elements of the organisation's operation. Securing your business goes beyond just implementing some firewall rules, anti-virus software and data backup solutions. Today, it requires a comprehensive programmatic approach.

Being compliant with standards might protect you from litigation, but will it ensure you are fully protected and your business safe?

Infrastructure Security Audit

An Infrastructure Security Audit evaluates the security of a company's information system by measuring how well it conforms to a set of established criteria.

Running such an audit on a regular basis helps organisations identify internal network vulnerabilities.

The bigger your company is, the more likely it is that there is a moral and even legal requirement to undertake regular audits. No matter what size, an external assessment should be conducted to minimise your chances of being one of the 57% of companies that security specialists expect to be breached next year.

THE TRILOGY APPROACH

Our approach starts with a deep audit and analysis of the full IT infrastructure.

We then provide a customised plan to implement solutions to tackle exposed areas in the short-term and more comprehensive protection in the medium and longer term.

Finally, a proactive security management regime is recommended.

BENEFITS

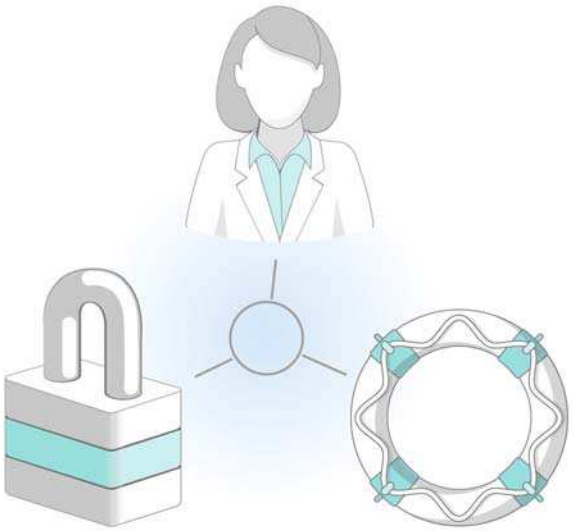
The average data breach takes 210 days to be detected. Just think about how much damage that will have caused before you even are aware. An infrastructure security audit sets you up to help prevent breaches by finding areas where you may be exposed. It also enables you to:

- Find the vulnerabilities before they find you
- Protect your company
- Be compliant with EU data protection regulations

How does a Security Audit work?

Trilogy site visit

Our approach starts with a deep audit and analysis of your full IT infrastructure by a member of Trilogy Technologies' security team. By means of a systematic, measureable technical assessment of the environment, the audit process will include vulnerability scans, examination of system settings and patch levels and interviews with key personnel to understand management security controls.



Employee network access is one of the most frequent issues Trilogy uncovers. This includes something as simple as forgetting to remove employee access after they have left the company. Some other common and easily fixed issues we find are:

1. Password policy review
2. Removal of unauthorised software such as LogMeIn, TeamViewer and GoToMyPc
3. Enforcing data loss protection action items including USB lockdown and removing Dropbox access
4. Updating or upgrading firewall and server firmware

This provides our consultant with the required information to build a customised plan to identify a series of recommendations.

Security Audit Report

Post audit and analysis, which may take up to a week depending on the scale of the infrastructure, you will be provided with a report categorised into three areas:

1. **Red** — Significant issues that require corrective action to meet business objectives.
2. **Amber** — Problems with a negative effect, however not deemed critical. Action should be taken to resolve or monitor.
3. **Green** — Area performing to plan.

Addressing the red and amber action items assist in mitigating the entry points for a targeted attack.

Being compliant with standards might protect you from litigation, but will it ensure your business is safe and you are fully protected?

By taking this approach, organisations can quickly identify a clear roadmap and start a continuous journey of proactive protection for the business.

DUBLIN OFFICE
Tel: +353 (0)1 476 8050

LONDON OFFICE
Tel: +44 (0)20 7440 6500

info@trilogytechnologies.com
www.trilogytechnologies.com