SAEPIO
INFORMATION SECURITY

DATASHEET

Saepio Information Security Audit

If you don't know where you are right now, it's almost impossible to work towards a destination. This is something Saepio see regularly. Our customers want to improve their security posture and to reduce risk, but they're unsure where to begin.

Regardless of where you are from a security maturity standpoint, understanding your current Baseline is key to making improvements.

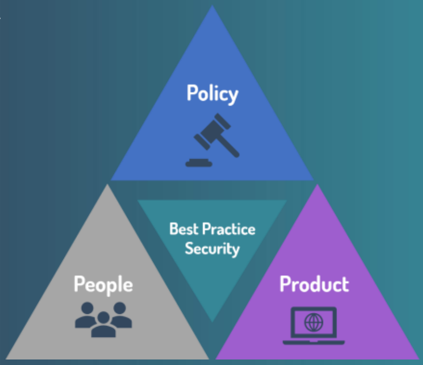
Saepio believe the best way to kick off the process and to establish your **baseline** is to conduct an audit of your existing security policies, processes and controls, against a compliance standard or best practice framework. We call this your 'Security State of the Nation'. Key stakeholders are interviewed. Existing security infrastructure is documented. Risks are quantified. Recommendations are made for how you will move forward to achieve your target state... but what is your target state?

In a post GDPR world, organisations you work with, or who are in your supply chain are looking to insulate themselves from a PII related data breach. As there is no formal GDPR certification, UK organisations are looking to **"Best Practice Frameworks"** to help demonstrate that they are taking Information Security seriously, In the UK there are two that are commonly used as a benchmark:

NCSC Cyber Essentials Plus & ISO27001

ABOUT SAEPIO?

Saepio is an Information Security advisor that helps organisations reduce their cyber risk and improve security posture.



Saepio believe security is more than technology. Best practice policy and process direct a successful security strategy. Products and people help to enforce it.

NCSC Cyber Essentials Plus Framework

5 core technical controls of Cyber Essentials Plus

- Secure your internet connection
- Secure your devices and software
- Control access to your data and services
- Protect from virus and other malware
- Keep your devices and software up to date

ISO 27001

5 benefits to achieving the certification

- Help retain business and win new customers
- Improve internal processes
- Help comply with other commercial, compliance or legal requirements
- Avoid data breaches (and the potential fines they might bring)
- Protect your reputation, and brand image

Organisations who have already adopted ISO27001 will find that Cyber Essentials maps to their existing systems, but ISO27001-compliant organisations will still need an additional assessment to verify compliance with Cyber Essentials Plus.

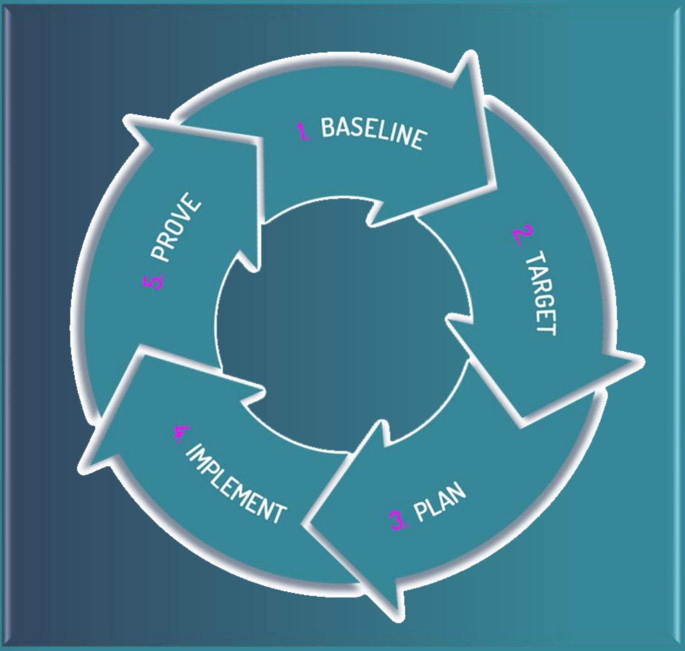
Our Approach

Our typical approach is to Baseline against both frameworks.

Cyber Essentials Plus is a great place to initially Target, it covers the fundamentals and provides the foundations for risk reduction and security improvement.

Using ISO27001 to map where you are, gives a best practice snapshot of your existing state, setting the bar high and giving you areas of improvement to fall in line with the standard.

Even if certification against ISO27001 may not be something you ever need to undertake, it still makes sense to map where you are and Plan future improvements against it.



> "Going through the Cyber Essentials Plus Gap Analysis audit from Saepio has been really helpful to us. It's confirmed the positive work we had already been doing, and has highlighted some areas for us to focus on. We've made some immediate improvements and now feel confident to proceed with the testing to obtain Cyber Essentials Plus certification." CISO, UK Insurance Firm

What are the outputs of the process?

- High level RAG management report
- High level prioritised security improvement plan
- Detailed Cyber Essentials Plus assessment
- ISO27001 Statement of Applicability working document*
- Creation of a customised Risk Register
- CIS top 20 critical controls security infrastructure review

Moving forward post Gap Analysis

Once an Audit has been completed, the Baseline established, and the Target identified, the improvements can begin. The Plan will look at Policy, Product & People, ensuring the work is directed towards risk reduction and the overarching best practice or compliance standard. Saepio can assist with Implementation of the plan through one of our experienced virtual CISOs if required.

If the end goal is to Prove what you've been doing, and be formally awarded a best practice certificate, Saepio assist by making sure you are in a position of readiness prior to the audit with the chosen accrediting body.

To learn more about the process and how it can help you increase your awareness, quantify your risk and provide you with a framework for Continual Security Improvement, please get in touch with either your Saepio account manager, or the Saepio solutions team.