Cyber Essentials 'Pathways': From experiment to proof of concept

We are encouraging large organisations to help us develop an alternative route to certification.

Anne W

When Chris Ensor described the Cyber Essentials 'Pathways' experiment, he promised that I'd follow up with a blog that explains what this means in practice, and what we're doing next....

What is the Cyber Essentials 'Pathways' approach?

As you probably know, the Cyber Essentials technical controls have been carefully defined to protect against the most common types of cyber attack. But as Chris said, there are sometimes legitimate reasons why an organisation can't implement some controls. In these cases, the organisation may have other mitigations in place.

To gain Cyber Essentials certification via the 'Pathways' route, an organisation will need to demonstrate they have alternative technical controls to those prescribed which will enable them to meet the overall intended *outcome* ; that is resilience to a 'commodity attack*'.

The Certification Body will test the alternative controls. Of course, this means the controls must be technical and testable. You cannot use an alternative control that states (for example) 'We have trained our users'.

The results of our Pathways experiment showed us that our original proposition was sound. It proved that it was feasible, via testing, to use an 'outcomes-based' approach to produce equivalent results compared to when using the original technical controls to achieve Cyber Essentials certification.

Moving from ‘experiment’ to Proof of Concept

However, just because something is feasible, doesn’t make it practical. For the Cyber Essentials Pathways approach to work outside of a carefully managed bespoke experiment, we need to demonstrate that we can package it in a way that is repeatable, scalable, and commercially viable. We now plan to explore this via a 12-month Proof of Concept (PoC) phase that we hope to launch over summer.

Over the next few months, our delivery partner IASME will be developing the structures, processes and materials necessary to run this PoC. These will include:

- establishing the participation criteria for potential Certification Bodies and Assessors
- developing the certification pass/fail criteria
- recruiting Certification Bodies to participate
- developing guidance for both Certification Bodies and their potential clients

As part of this approach, we would like to identify up to 40 large organisations (250+ employees) who are willing to pay to be part of the PoC. Participating organisations will work with their Certification Body through a 3-phase process that involves:

- a traditional Cyber Essentials self-assessment followed by Cyber Essentials Plus testing (resulting in either a pass or a gap analysis)
- the development of additional tests to verify the efficacy of alternative mitigations designed to result in the same outcomes intended by the specific technical controls (identified in the gap analysis)
- a testing phase and review, potentially leading to Cyber Essentials and Cyber Essentials Plus certification

The cost won’t be the same for all participating organisations. This is because the testing will take a different amount of time, depending on the infrastructure and the nature of the alternate mitigations that each organisation is using.

Based on our experiment, an average of 17 days of testing, moderation and assessment was required. But of course, that is an average; some will be quicker, others will take longer.

How to take part in the Proof of Concept

If you are a large organisation struggling to comply with the prescriptive nature of the Cyber Essentials technical controls - but have alternative mitigations in place that deliver the same outcome - we'd love to hear from you. If you would be interested in working with us on this exciting PoC, please register your interest via info@iasme.co.uk. We'll get back to you with all the relevant information you'll need, including in due course, how much this might cost.

Anne W
Head of NCSC Industry Assurance

* An attack from the internet that uses publicly-known tools and techniques.

WRITTEN BY

Anne W
Head of NCSC Industry Assurance

PUBLISHED

18 July 2024

WRITTEN FOR

Large organisations

Cyber security professionals

PART OF BLOG

Events and initiatives