Making Principles Based Assurance a reality

An update on the work to make Principles Based Assurance (PBA) usable in practice.

Duncan A

This article was amended in February 2025 to reflect the change to from a single PBA service to PBA based services.

Building on the initial PBA work

For some time now, the NCSC has been actively researching and consulting on the future of technology assurance in the UK. We first shared the outcome of this work in a 2021 white paper, which concluded that the chosen approach was Principles Based Assurance, or PBA.

To recap, PBA is a methodology that builds on NCSCs research and threat knowledge to present a universal, proportionate and risk-based approach so that users of a technology can gain confidence in its cyber security. A blog published alongside the white paper explains the background in more detail and why we opted for this approach.

There was a vibrant and constructive discussion about PBA at this year's CYBERUK event in Newport. The message we got was: "This sounds good, we like it and want it, but when will we see something tangible that we can use?" Or in other words: "What's the plan?"

Introducing PBA based services

The good news is we've made some progress and we plan to deliver a range of srvices that use PBA. These will be the precisely defined and tangible form of PBA that CYBERUK attendees were keen to see.

PBA based services are designed to be used by technology product manufacturers and those responsible for managing information and operational cyber risks when deploying technology. The key features and benefits of these services are:

- it assesses technology against structured principles and claims, based on NCSC research and our unique understanding of the threat
- using proven claims, argument and evidence (CAE) – more about that later – it makes building an assurance case repeatable and scalable
- the output is a clear statement of risk, not a traditional statement of compliance, that supports proportionate and informed risk management for users of the technology
- the CAE approach allows for generation of continuous assurance statements because it can be integrated into modern 'secure by design' engineering processes

---

What more can you say about PBA services now?

The NCSC will soon be publishing detailed information about the structure and operating model for PBA services. But before then, we'd like to share a couple of features now, to start engaging with the community. They are: the use of a new set of documents, called the 'Assurance principles and claims' (APC) documents, and the method and governance of how technology will be assessed.

What's an APC?

The PBA principles and risk-based methodology outlined in the 2021 white paper pointed to the various NCSC published Security Principles (such as those for cross domain solutions) and the new Assurance Principles as the starting point for assessing technology.

When defining PBA services, we recognised that the principles behind them, as published, aren't precise enough as a starting point for building a repeatable assurance case. So PBA services will use APC documents to do this.

An APC will restructure a set of already published security or assurance principles, formalising the language, and illustrating each individual principle with a set of ideal-scenario claims that, if met, means the technology solution is achieving what the principle intends. The NCSC will host the portfolio of APC documents.

For each individual technology product to be assured, it will be necessary to produce a claims document specific to that product. Those product-specific claims will be refined or enhanced claims from across the APC portfolio that are relevant to the product in hand. And for new products, it will be possible to propose alternative and different claims to those you'd find in an APC.

And the assessment and governance?

Once a manufacturer has laid out the claims for a specific product, it's time for the assessment. This means gathering evidence that either supports or rebuts each claim. The formal CAE approach used in PBA based services means that gathering evidence is unambiguous and repeatable.

If the evidence collected rebuts a claim, or only partially supports it, the assurance service will express this in the form of risks that the product hasn't proved it is managing. These risks would then need to be managed by the product users.

The services will support technology manufacturers to carry out their own self-assessment, but it will also allow for NCSC-approved assurance facilities to independently validate the evidence and risk statement. Where the evidence and risk statement have been independently validated, the NCSC will issue a certificate confirming they've been produced in line with proper process.

Next steps

We're already working with our partners to define and develop the technical details needed for services to operate. We'll also be communicating about the changes, and supporting manufacturers, assurance facilities and risk owners with these changes.

There will be a limited launch in 2023 for a small number of products so we can make sure that the process is robust enough to operate at scale. Learning from this limited launch, we'll then look to open up the service more widely from April 2024 onwards. In the meantime, look out for more about PBA based services on the NCSC website in 2023.

Duncan A
Principal Technical Director for Assurance

WRITTEN BY

Duncan A
Principal Technical Director for Assurance, NCSC

PUBLISHED

14 December 2022

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

Small & medium sized organisations

PART OF BLOG

Inside the NCSC