Principles Based Assurance (PBA)

Helping customers gain confidence that products are resilient to cyber attack.

1. What is Principles Based Assurance (PBA) and how will it help you ?
2. What technology is PBA for ?
3. When will PBA be available ?
4. What will PBA look like ?
5. Assurance, Principles & Claims (APCs)
6. Who does the assessment ?
7. Being able to make the right decision

What is Principles Based Assurance (PBA) and how will it help you?

At NCSC we are building Principles Based Assurance (PBA) to help our customers gain confidence that the technology they use every day is making them more resilient rather than more vulnerable to a cyber attack.

NCSC focuses its ‘hands on’ assurance effort on those technologies and customers that face the highest threats. Given how vast and connected the technology landscape is now, and how rapidly it is evolving, we recognise that there’s currently a gap in a UK capability to provide a trusted, accessible independent assessment of technology against the scaled threat model.

To plug this gap, we are building Principles Based Assurance, an NCSC framework for assurance best practice that we are planning to be scaled through industry partners to provide a consistent, accessible UK assurance service.

What technology is PBA for?

We’re not just looking at the functionality of *security products*, like firewalls or VPNs. Given how connected technology is now (to both other technology and people), we must include products (including software) whose primary function is not security, but a compromise of which would cause a significant impact.

We need to be able to consider different threat models the system needs to be resilient to. Critical National Infrastructure (CNI), defence and intelligence contexts are likely going to be up against attackers with significant resources, skill, and time, working in a targeted way. This is a different threat to attackers who leverage readily available tools and public vulnerabilities in a spontaneous and scaled way.

For many customers, gaining confidence that the technology they’re using is resilient to this latter threat model is all they require. If we come up with an approach that tries to make all technology resilient against the former model then timescales will extend, costs will rocket, and choice will vanish.

Like all other security products, quantum security products must follow PBA, as their goal – security – is the same.

Quantum security products and services offer “quantum advantage”.[1] The first quantum products to follow PBA will likely incur added 'first-mover' costs, which may also be accentuated by the need for some degree of re-engineering to enable evidencing of having met assurance claims. Hence it is likely that such products and services will initially find a market through protection of CNI and important customer (business, government and personal) data, required to remain secure long into the future, or other high value data.

[1] Refer to the “Introduction_Quantum Assurance” document.

When will PBA be available ?

Creating PBA can be thought of as a three-layered process.

The first, foundational, layer is the **philosophy** of a risk-based rather than a compliance-driven approach. The second stage is developing a consistent **method** that can be followed, along with documentation and templates to be used. The final stage is how the method can be deployed and accessed as a **service** in the marketplace by both vendors and buyers in a consistent and trusted way.

Service

PBA needs to be accessed by both vendors and buyers in a consistent way both through trusted industry services to provide independent assessment, capability, or through the NCSC website.

Method

PBA needs a well-structured approach that both enables vendors to demonstrate evidence against it and provides consistency in the way in which industry and government deploy it as a scheme or service. It is defined by a framework, documentation and technical standards approved by the NCSC.

Philosophy

PBA is an assurance philosophy stretching across the whole customer spectrum. It promotes a more adaptable and holistic, threat-first approach. with understandable outputs that help people to make risk-based decisions. More detail on this aspect is in the White Paper.

The NCSC will be publishing the PBA method, when it is available, so that people can start using it.

Work is about to begin on the Service layer, to design a way to scale the PBA philosophy and method through Industry partners. By next year we plan to have an embryonic network of approved Cyber Resilience Test Facilities.

What will PBA look like?

On our Technology Assurance section of the website, you will find our Core Technology Assurance Principles. These principles describe the security outcomes that we'd look to assess against to gain confidence in any product. They are divided into three pillars:

1.

Development

an assessment of the security of the vendor and where appropriate this would include the security of the development environment. Find out more about the 7 principles underpinning the development of secure products.

2.

Design & functionality

an assessment of the resilience of the product to cyber attack and the efficacy of any security functionality. Find out more about the 6 principles for design and functionality.

3.

Through-life

an assessment of how well the security of the product or service will be maintained during its operational lifetime. Find out more about the 5 principles for maintaining a product's security through all stages of its life-cycle.

Versions of the three NCSC pillar documents, with added (highlighted) quantum-specific comments, support this PBA document.

Assurance, Principles & Claims (APCs)

To enable people to evidence and assess against these principles in a consistent way, we are generating a set of new artefacts called Assurance, Principles & Claims (APCs).

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.

It is based on Claims, Argument, Evidence (CAE) approaches used for safety assurance, tailored for cyber security assurance. Full technical specifications for this approach will be published by NCSC, but we can illustrate the concepts with this simple flow:

Claim

A claim is a true/false statement about a property of a particular object. A claim is exactly what you might consider it to be from common usage of the term; an idea that someone is trying to convince somebody else is true. As an example a product may intend to be able to recover itself from compromise, leading to a claim such as “The Product protects itself from persistent compromise”

Argument

An argument is a rule that provides the bridge between what we know or are assuming (sub-claims, evidence) and the top level claim we are investigating. In the example above an argument would begin this bridging by breaking down the claim we are making into a number of sub-claims that are more easily evidenced; one example would be to decompose the claim into sub-claims that describe the what the term “protect” means, such as “The product detects and acts on compromise within 2 seconds” and “When compromise is detected the device stops operating”.

Evidence

Evidence is an artefact that establishes facts that can be trusted and lead directly to a claim (via an argument). There can be many sources of information but what makes one evidence is the support or rebuttal of a claim. To continue the example the sub-claims described could be evidenced by an independent test facility deliberately launching various forms of compromise against a device and observing the time until the device responds, and the operational state of the device upon that response.

For particular technology classes, where there is an identified need, bespoke APCs will be created. The NCSC will host the whole portfolio of APC documents on its website, so that vendors and customers can access both core APCs and the bespoke APCs according to their needs.

The “Introduction_Quantum Assurance” document forms the basis for these comments and should be read first. The CAE scenario for quantum secure communication products is that their “quantum advantage” follows from a security proof (the claim). If this is composable, it can comprise various components (sub-claims). The argument follows that the security proof can be applied to a particular quantum security product, provided that there is evidence (through a set of measurements applied to the hardware) that the product satisfies all the physical assumptions that are specified in order to construct the security proof.

If the measurement result evidence demonstrates discrepancies between the actual properties of the hardware and those assumed for the security proof, these discrepancies form quantum side channels, which might be exploited to circumvent the security. Countermeasures are required to prevent such attacks. Example countermeasures for QKD are discussed in section 5 of the “Principles: Product development” pillar document.

The security proof claim is directed towards a device whose functionality is to enable security through quantum means. This device is likely to be an element of a larger product, or integrated into a technological system such as a communications network, that is providing the required secure service to customers. Hence the claim for quantum advantage is likely to be only one of many sub-claims for the larger system and, as described above, may itself be composable from further sub-claims.

Who does the assessment?

How much confidence you need in the assessment of the product will probably depend on the impact of something going wrong.

If the criticality of a product is high or you don’t have the skills to do the assessment yourself, then an independent assessment might be a more appropriate route to gaining confidence in a product’s cyber resilience. If the impact would be less serious, then a self-assertion against the relevant APC document by the vendor may be sufficient (and less costly).

PBA enables flexibility in the route chosen to gain confidence, but consistency and structure for the outcomes and evidence that need to be demonstrated.

Quantum knowledge and equipment is required to generate the evidence that a quantum security product does indeed satisfy the physical assumptions specified for its “quantum advantage”. For some applications and technologies, it may be that supplier-generated evidence is sufficient for a user. However, in many cases it is likely that independent assessment of the quantum security product is appropriate and desirable. There is a strong case for a body being established to support (particularly small) companies with assurance of the quantum specific aspects of their products. Without such a body, UK companies focused on quantum security products will individually encounter a very substantial assurance workload to gain market entry[1].

[1] For an expanded expression of this point, refer to the “Introduction_Quantum Assurance” document.

Being able to make the right decision

Ultimately, PBA needs to enable a customer to make an informed decision about whether to buy the product or how to integrate it into their system in a secure way. The outputs should be usable and accessible by all kinds of customers, many of whom will not be security experts.

A PBA Assurance Statement (from an independent assessment) will shine a light on what cyber security properties a product has, and how this impacts the risks of the system it’s integrated into.