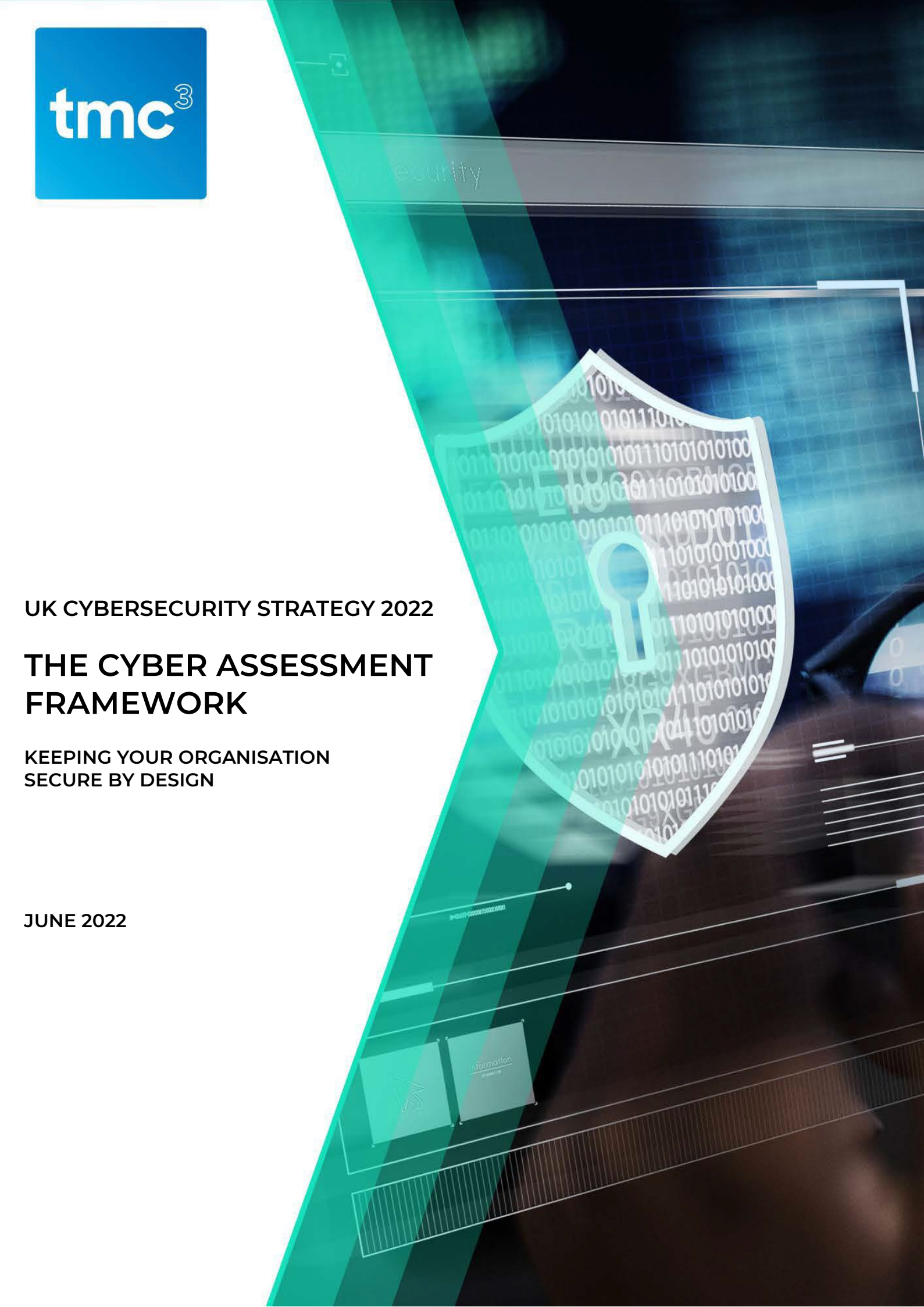


UK CYBERSECURITY STRATEGY 2022

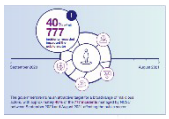
THE CYBER ASSESSMENT FRAMEWORK

KEEPING YOUR ORGANISATION SECURE BY DESIGN

JUNE 2022

what's covered inside

Introduction to the UK Cyber Security Strategy 2022



What does it look like to achieve?

Strategic Pillars – aims of the strategy.

The cyber assessment framework – objectives, principles, and outcomes.

Getting support from tmc³ – your trusted partner.

introduction to the strategy

The word strategy has often been used as a synonym for "…we were going to get around to it at some point, but…", as part of a get out clause when a serious problem had already manifested itself – often with dire consequences.

Protecting our most valuable assets cannot be an afterthought. The threat exists now and the UK must rise to the challenge and meet this problem head-on.

The days of a disjointed approach to information and cyber security are over. Ad-hoc solutions, rushed into production and focusing only on the technical, are now woefully unsuited to the task. We hear with increasing regularity of organisations suffering breaches, often ones hosting our most intimate information.

This problem isn't going to subside. As our reliance on digital services grows, so our threat landscape expands – the tempting prize of personal data is too lucrative a reward for a cybercriminal.

This isn't a criticism of any one department, far from it; great strides and efforts had been made in recent years to better defend ourselves against an ever growing army of threat-actors. But as history has taught us time and again, warfare, including cyber-warfare, doesn't wait for both sides to catch up. The enemy will seek out your weakest link and expose it.

And when that link has a social media account, or doesn't understand that the email they have just opened may not be from who they say they are, what do we do? There's only so many holes a single department can plug.

What's needed is a unified and integrated approach to our information security – one understood by everyone. We need mass buy-in to the ***culture and awareness*** of good security – not just a prescriptive list of access-control rules for Mike in IT. More than that, the industry needs leadership. A rally point. And it needs to be future proof. If we accept where we are, and uniformly agree where we need to be we can throw the protective net of information security practices over the whole country.

So who, or what, will guide us through this grand endeavor? The UK National Cyber Strategy 2022.

Understanding that we live in an everchanging world, the strategy sets out the governments' commitment to remaining protected and viable in the digital age well into the next decade. It represents a change in culture – one that accounts for the intrinsic value of information, and how its protection must be budgeted for as part of a business strategy – and not something bolted on as an afterthought.

In short, the UK will brand itself as a well-resourced cyber-power on the global stage – and stay there.

what does it look like to achieve?

Of course, talk is easy, albeit rarely cheap. So what does it actually mean to have a "national cyber strategy"?

This paper isn't here to regurgitate the information contained in a publicly available document – but it would be wise to at least highlight some of the more specific ambitions, including the timescales the sector will be working towards.

The vision, which aims to harden UK Governments' departments against a growing number of cyber-threats – whilst remaining a global player on the technology scene - may come across as an attempt at policy crowd pleasing. But unlike previous cyber security pledges and strategies – this strategy goes on to explain ***how*** they're going to achieve it.

Laid out in an (almost) step-by-step fashion, the strategic pillars are used to offer an overview of the direction (or more accurately the change in direction) central government needs its departments to take.

This has been driven, in no small part, by the fundamental changes in attitude to cyber security alluded to earlier. With each passing day the arsenal of weapons in the hands of would be attackers grows. As hostile foreign powers invest heavily to find new attack vectors, so the borders we need to defend become more vulnerable.

Of course, enhancing our cyber-profile isn't only about protecting ourselves from hostile forces. There's 21st century global stage out there – and if we want to be a player, we have to understand the game. UK PLC needs to keep up with the jones'.

It's clear that what's really changed is the awareness of just how big a task we have – and now we've accepted that we need to build upon it.

There may be those who think this doesn't affect them. Some may not work in or with central government. There may even be those that do work in those areas thinking it won't impact them. It will. In fact, it already does.

To those who don't work with central government - can you be sure you never will? Consider the answer carefully.

Working "with" doesn't always mean you sit in Downing Street. Your organisation could be a supplier, or a downstream supplier of their primary contract holders.

This strategy is far reaching – a Secure by Design organisation will look to understand, in detail, how its processes and components are sourced and secured – hiding behind an ISO accreditation won't cut it now.

Indeed, the word accreditation is itself something of an archaic term. This strategy de-enriches the responsibility away from the certified few and into the hands of the departments themselves. Giving them the tools, skills, and support needed to define their own profiles.

Organsations across all sectors need to start preparing for the changes. The National Cyber Security Centre has a wealth of information from many sources. Start early - cybersecurity is never finished.

strategic pillars

Understanding the amount of work required to adopt a framework can be a daunting task. It would therefore be useful to consider the aims – or pillars – to better understand the spirit of the task – and how they can be tailored to work with, not against, your organisations current processes.

The keyword of this pillar is ***organsational.*** What's more, it's here we find evidence to support the claim that responsibility of cyber defense is moving away from a prescriptive system of formal accreditation, by de-enriching accountability to individual departments who, guided by subject experts from across industry, are now able to assess themselves against a unified standard to understand their own profiles. This common approach offers a stability rarely seen in industry – an opportunity that must be taken with an enthusiasm equal to the size of the task.

Essentially, Pillar 1 represents the foundations of a Secure by Design organisation. Understanding that the decisions and behaviours of one department have consequences for the next, and that security controls cannot work efficiently when siloed. Rather they exist to inter-connect and refer to each other to offer a broader level of security – if applied correctly.

Fortunately, this pillar isn't simply left out there without any amplifying information. Far from it. It goes on to explain ***exactly*** how it plans to achieve this organisational resilience – by introducing us to the Cyber Assessment Framework (CAF).

It would be wise to get used to that abbreviation – CAF. Given that this strategy's vision goes out to 2030, so the work of rolling it out intensifies. Already at version 3.1 (correct at time of writing) – its adaptable framework of objectives, principles, and indicators of good practice (IGPs) are already being integrated by government departments. ***Those not considering its implementation now may find themselves in a difficult position as the decade marches on.***

In truth, there's no reason to not get involved early. With the appropriate support, it's non-prescriptive IGPs are designed to complement the controls of other frameworks – although its inescapable similarities to the NIST Cyber security Framework (CSF) may make that the obvious partner-framework.

With IGPs ranging from what Top Management need to establish in policy, to Managing Risk in the Supply Chain. From Physical Security to Promoting Cyber security Culture and Training; the CAF covers it all.

Pillar 2 may appear something of an afterthought, dwarfed by the enormity of the objectives found in Pillar 1. No new framework to be found here. But consider the implications of the statement – Defend as One. What does this actually mean?

It means coherence. Across government, between departments, between management and their policies, and the IT desk agent taking calls to unlock user accounts. Suddenly Pillar 2 looks a great deal bigger than Pillar 1.

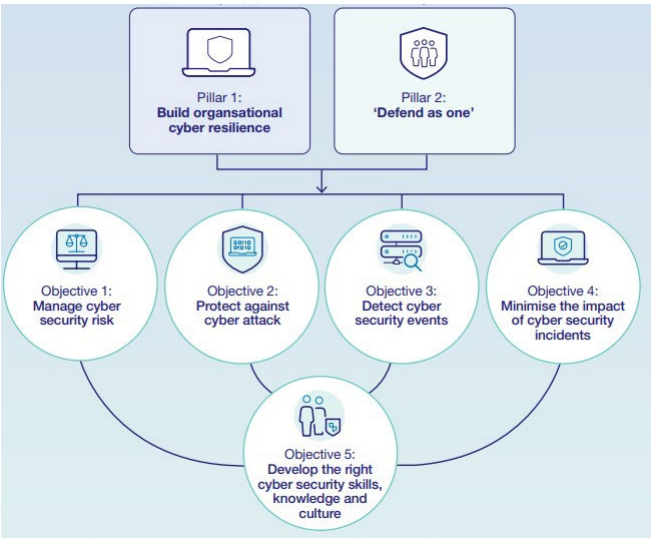
It's here that we begin to understand the holistic nature of this strategy. We are provided the tools in the CAF – with its use of generic IGPs that are designed to be ***interpreted*** and ***adapted;*** not stuck to rigidly with a one-size-fits-all attitude.

We are given the freedom to adapt the framework as needed and fit it round the controls of others, with the comforting support of the NCSC's with its useful links to international information.

And finally, united we stand behind the guidance and drive of the Government Cyber Coordination Centre (GCCC) whose task it will be to oversee the efforts and actively engage with and prosecute opportunities in support of Pillar 2.

the cyber assessment framework

If the pillars are the aims of the strategy – then the CAF is the direction. Understanding how to use this in a practical sense will be crucial.



It's worth repeating at this stage one very important fact; ***the CAF is not designed to replace an existing framework – it can, indeed should, be integrated alongside existing policies and controls to enhance your security profile.***

So how exactly does an organisation achieve that? Let's take it step by step.

objectives to support the strategy

The first task for any organisation should be to orient themselves and establish their "as-is" profile. Doubtless there will be professionals out there with a delightfully complicated abbreviation of what I mean, but I'll keep it simple:

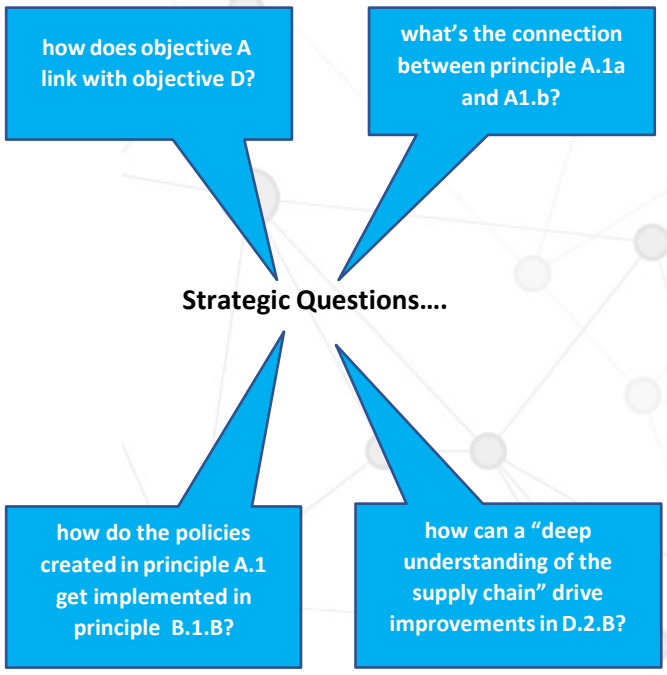
Sit down, take five – and look at the four objectives of the framework.

I realise this may seem a gross simplification of an important task – and it is. Deliberately so. This is only the first stage – and in truth it's about getting acquainted with the CAF. Having taken this breath, we permit ourselves a moment to digest the governing objectives:

- ***Objective A: Managing Security Risk***
- ***Objective B: Protecting Against Cyber-Attacks***
- ***Objective C: Detecting Cybersecurity Events***
- ***Objective D: Minimising the Impact of Cyber security Incidents***

The simplicity of the objectives belies the scope of their implementation. I would argue, however, that understanding how the CAF objectives align with the strategy is a rather good start. What's more, assuming this stage has been approached dynamically, questions from across the organisation - interested parties and stakeholders alike - will have been collated which will prove useful as the process continues…

Note I say questions – not answers. Top-management should be encouraging their teams to question the process from the start, actively promoting the culture of security so critical to the strategy:



These questions haven't been added for dramatic impact. They are ***fundamental*** to the proper adoption of the CAF and ultimate alignment with the strategy. The importance of a holistic approach cannot be overstated – siloes of individual controls will not work.

Outcomes and Principles

Reviewing the objectives will uncover the true substance of the CAF. And importantly, it won't take long before it becomes clear how the CAF is to be used.

Interpreting outcomes, guided by indicators, will describe what a desirable practice would look like – not ticking boxes on checklists.

<table>
<tr><th colspan="4">Objective A</th></tr>
<tr><th colspan="2">Principle A1</th><th colspan="2">Principle A2</th></tr>
<tr><th>Outcome A1.a</th><th>Outcome A1.b</th><th>Outcome A2.a</th><th>Outcome A2.b</th></tr>
<tr><td colspan="2" rowspan="3"><u>Indicator of Good Practices (IGPS)</u>

Support and Guide to achieve the outcome.
→</td><td colspan="2">Answer yes from here and outcome is not achieved</td></tr>
<tr><td colspan="2">Display all these characteristics for full compliance</td></tr>
<tr><td colspan="2">Processes that add value to security but not fully compliant</td></tr>
</table>

As the image shows, ***objectives*** are supported by ***principles*** covering everything from Resilient Network Design to Proactive Attack Discovery. Principles are further divided into ***outcomes***; each containing convenient guides (Indicators of Good Practice) of what a full suite of good processes in a specific domain would look like.

It's this layered approach that sets the CAF apart from previous strategies. There are no claims of ground-breaking innovation – it isn't conceptually any different from the practices described in the (many) papers surrounding Defense in Depth – but it's the first time the UK Government has truly recognised the need for inter-departmental uniformity.

IGPs and their application

IGPs could be justifiably considered the most critical part of the framework. As the foundation they are the bedrock that supports an architecturally secure network. It is here that the skills of a cyber security professional will be tested – with investment in the right level of experience seeing an immediate return on investment through the efficient integration of the CAF

with other models, a process critical to eventual compliance.

IGPs are, broadly speaking, laid out in 3 distinct categories and conveniently colour coded in the lingua franca that is the traffic light system:

What's bad, What's good, What's on track

I should take time to point out that the NCSC doesn't use these terms. But they do advise to take an interpretive approach to the CAF – and I admit to using this advice somewhat liberally, with good reason.

Officially speaking, the IGP categories are:

Not Achieved, Achieved, Partially Achieved.

For context, the red "non-compliant" IGPs are simple; answer yes to **just one** of the questions and you cannot be compliant with the outcome.

Likewise, answer yes to an IGP in the green section then you are justified in claiming conformity to that process, behaviour, or policy – and have satisfied an element of that outcome. Answer yes to all of the IGPs from this section and you will have achieved that outcome, achieve all the outcomes in a principle, and all the principles, to achieve the objective of that domain.

Again, the holistic nature of the framework needs to be considered. With appropriate professional support, organisations can develop a set of applicable IGPs that are relevant to their business objectives and industry sector, working towards them iteratively for full compliance.

The benefit of this approach will be not falling foul of the non-conforming IGPs by default – you can't answer "yes" to a red if you're displaying the behaviors of the amber or green – this section satisfies itself!

I should note one word of caution – this suggestion isn't to downplay the importance of the red IGPs; rather to use them as a tool at the end of the process – a final sanity check to satisfy oneself that they are not displaying any non-conforming characteristics.

You'll note I left the ***What's on Track*** section to last. With good reason – this area is defined as being an indicator of ***some*** of the behaviors expected, albeit falling short of being perfect. They still, however, contribute to the overall security posture – a perfectly acceptable position if this suits the appetites of the organisation.

I want to finish this section by acknowledging there may be some academic disagreement with how I've presented this information. Allow me a moment to justify my reasoning.

Having studied the CAF and Strategy at length to absorb the spirit as well as the technical details, I find myself taking issue with one area – IGP terminology.

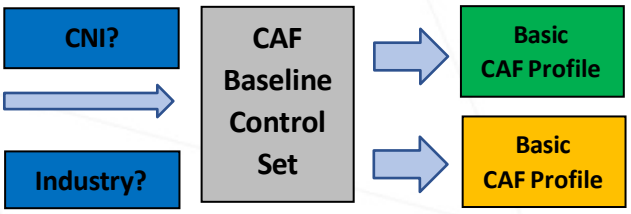
For the vast majority of the strategy, we are introduced to a new, dynamic approach that aligns the UK Cyber- Position with the 21st Century. Changes that will see a more granular system of accountability that promotes behaviour and culture, without being overly prescriptive.

Why then, imply a pass/fail test condition with words like "achieved" and "not achieved" that might result in a stressed, rushed, hastily applied set of security controls?

As a Cyber security professional I see far more value in starting this process on a positive footing – choosing what fits, modifying it to suit our objectives, striving for improvements that will see compliance with the green IGPs across the board – but cognisant of the fact that may never happen. Factors outside the organisations control – budgets, resources, regulatory and legal requirements – may stop it. Management may even accept partial compliance of certain objectives if that status falls within their tolerance levels.

Regardless, it should be the duty of all Cybersecurity professionals to strive for improvement within the bounds of available resources; not the framework to say whether we've passed or failed.

Profiles based on CAF Outcomes



There will never be a process that suits all organisations. Cyber security is too complicated a discipline embedded into the myriad businesses that make a digital economy.

One step that will help all businesses, however, will be establishing their ***current profile vs their target one***.

The strategy sets out two conditions. Departments deemed to be essential in delivering critical functions will need to achieve an ***"enhanced"*** CAF profile by 2025 – with all departments required to meet the outcomes of their profiles by 2026. Any other government organisation will need to achieve a ***"basic"*** CAF profile by 2030. The exact requirements, or baselines control sets, are somewhat lacking in detail.

It would make sense that each profile will be properly assessed based on the inherent and potential risks, on a per-industry or sector basis. Indeed, by that logic one could make some reasonable assumptions as to which category they will fall into.

And is it coincidence that the CAF allows for a partial compliance in certain outcomes? It's a safe bet being that a department requiring an ***enhanced*** profile will have to "go green" across the board – with less critical areas given the freedom to set a lower baseline.

Only time will tell on the specifics of profiles, with logic dictating which department falls into which category. We need to accept that the CAF is in its relative infancy, with new guidelines and compliance information appearing on the NCSC website regularly.

What is clear is the departments actively engaging with the strategy are already seeing the benefits. Starting with a robust gap analysis, organisations with the forethought to invest now have already established their current profiles against the CAF – with a common sense approach dictating what their likely target profile will be.

And to date I haven't worked with any organisation – regardless of size or perceived criticality – that has set themselves a target what could be called a "basic" profile. Nor would I advise to do so without good reason.

Engaging the services of an company like tmc³ means your security will be appropriate - never basic.

references and useful links

UK Government Cyber Strategy

NCSC CAF Guide

NCSC General Guidance

NIST CSF Guide

tmc³ - here to help

tmc³ have established themselves as *the* go-to provider of expertise for cyber and information security solutions across the public and private sectors.

Its dedicated team of experienced security specialists are on hand to guide your department through this period of change – ensuring you not only comply, but thrive in the digital era.

With an innate understanding of the industry, our comprehensive suite of solutions ensure your business objectives are enabled by security solutions – not hindered by them.

From bespoke mapping tools to support gap analysis, to informal spotlight sessions for your teams – we understand that promoting a culture of security is more than just a technical process, it's a way of life.

With innovative approaches, tmc³ will scale your security posture to meet the demands of UK Governments Cybersecurity Strategy 2022, integrating it seamlessly with your current controls, and ensure your compliance now – and in the future.

LETS START THE CONVERSATION

visit our website

email us

call us : +44 (0) 113 873 0449

Authored by Dave Kennedy, Consultant at tmc³