CLOUDGUARD
Security Done Different

January 2025

Updated 30 January 2025

Understanding the NCSC Cyber Assessment Framework

Table of contents

3 What is the Cyber Assessment Framework (CAF)?

6 CAF objective A: Managing security risk

7 CAF objective B: Protecting against cyber attacks

9 CAF objective C: Detecting cyber security events

10 CAF Objective D: Minimising the Impact of Cyber Security Incidents

11 What makes the CAF so good?

12 A quick word on CAF profiles

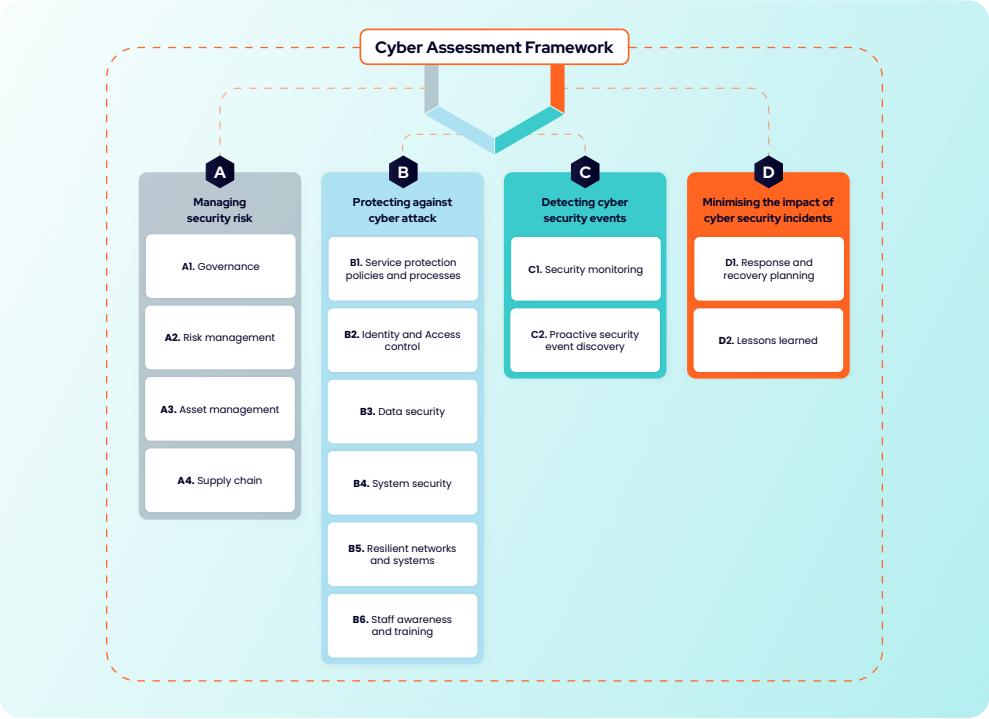
13 9 steps for getting started with the CAF effectively

14 Wrapping up this guide to the Cyber Assessment Framework

What is the Cyber Assessment Framework (CAF)?

In its simplest form, The Cyber Assessment Framework (CAF) is a way of assessing if your cybersecurity measures are strong enough to manage risks and protect your critical systems, as well as improve your organisation's resilience and ability to respond to threats.

The Cyber Assessment Framework (CAF) was created by the National Cyber Security Centre (NCSC). You might hear it called 'common CAF,' 'core CAF,' 'pure CAF,' or 'vanilla CAF,' as it's the original, sector-agnostic version.



The CAF helps you understand how well your organisation is managing cyber risks, especially for critical operations that need to keep running smoothly.

It provides a structured way to assess your cybersecurity. This can be done either through self-assessment or with the help of an external expert.

It's important for me to note that although the CAF includes the word 'cyber,' it's broader than what many people or organisations typically associate with cybersecurity.

It covers areas like information risk, information security, and the people, processes, and technology involved. It's not just about IT and technical systems. It takes a more comprehensive view of resilience.

Unlike a simple checklist of tasks, the CAF focuses on outcomes your security should achieve.

The main benefit? It ensures your organisation is as prepared and resilient as possible against cyber threats.

How is the CAF is structured?

I'll provide you with a quick breakdown of each section of the CAF but here is the overall structure.

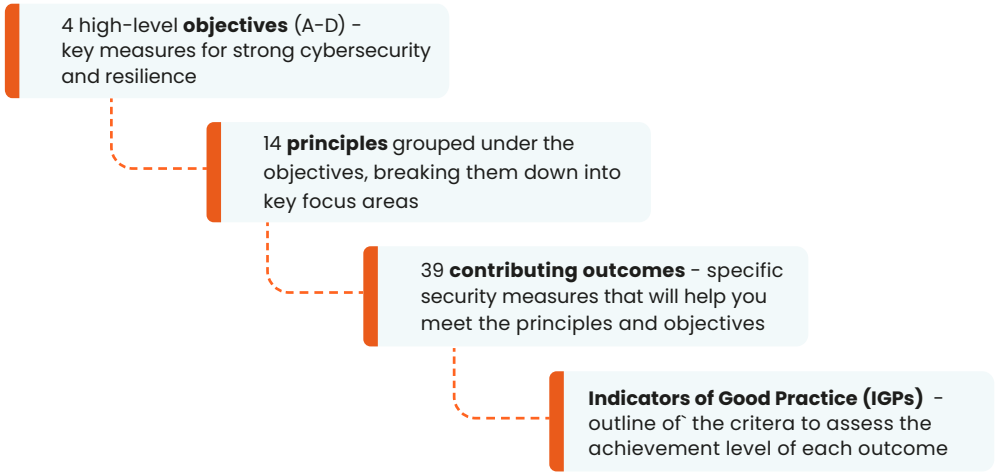
NCSC Cyber Assessment Framework v3.2 structure

Objectives (4): The top-level goals your organisation should aim to achieve for cybersecurity and resilience. They provide the overall direction for security efforts.

Principles (14): Broad areas that support each objective. Each principle helps guide you on how to achieve the objectives through specific focus areas.

Contributing Outcomes (39): Specific security measures tied to each principle. Achieving these outcomes will help you meet the principles and, in turn, the broader objectives.

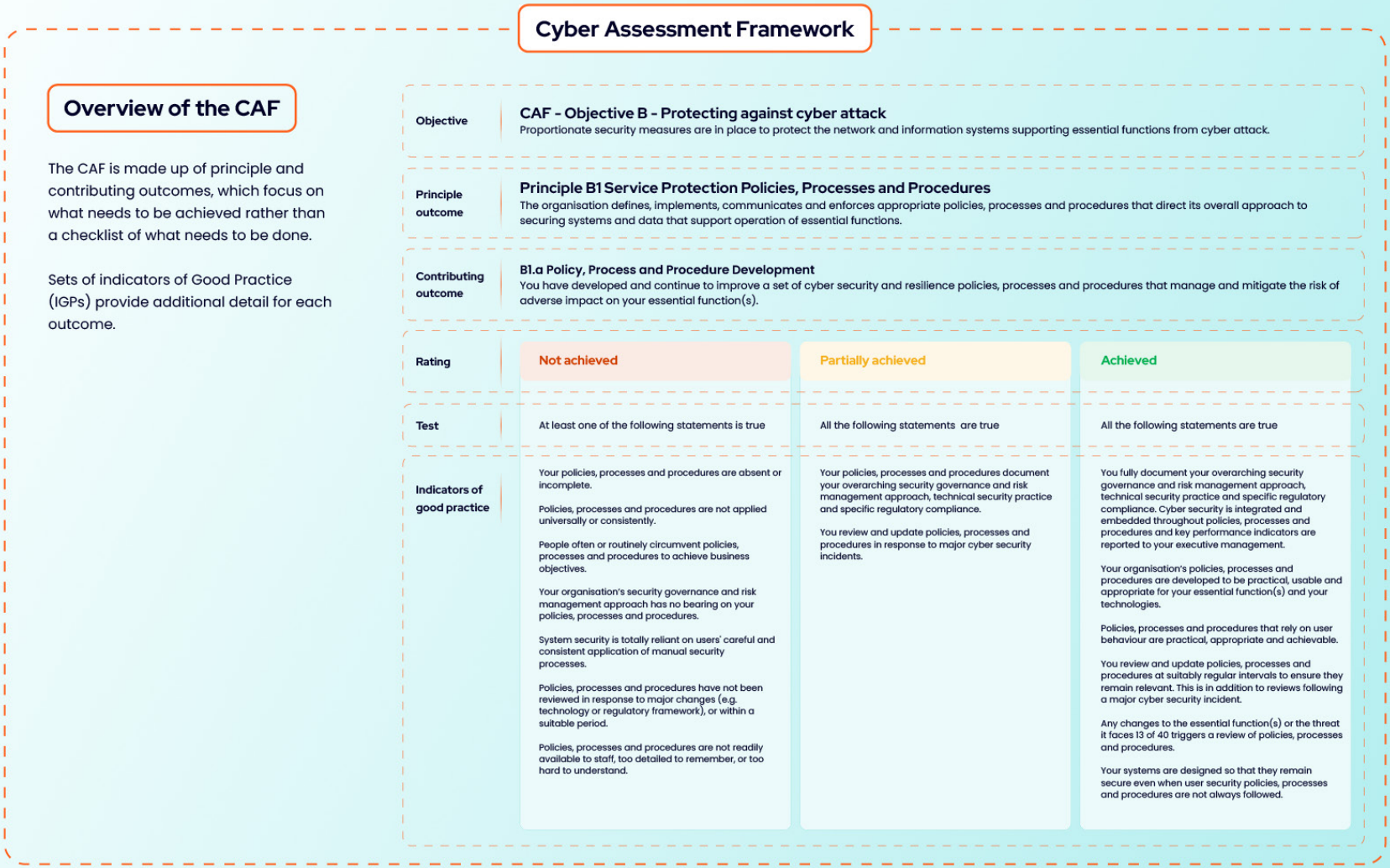
Indicators of Good Practice (IGPs) (varies per outcome): Detailed criteria for you to assess whether a contributing outcome has been Achieved, Partially Achieved, or Not Achieved, helping you determine how well your organisation is meeting each contributing outcome.



IGPs are intended to help inform your expert judgement, provide important examples for what you'll need to consider and are widely applicable across different organisations (though you should confirm their applicability).

IGPs are not a rigid checklist for you to follow, an exhaustive list of everything to consider or guaranteed to apply exactly to your organisation.

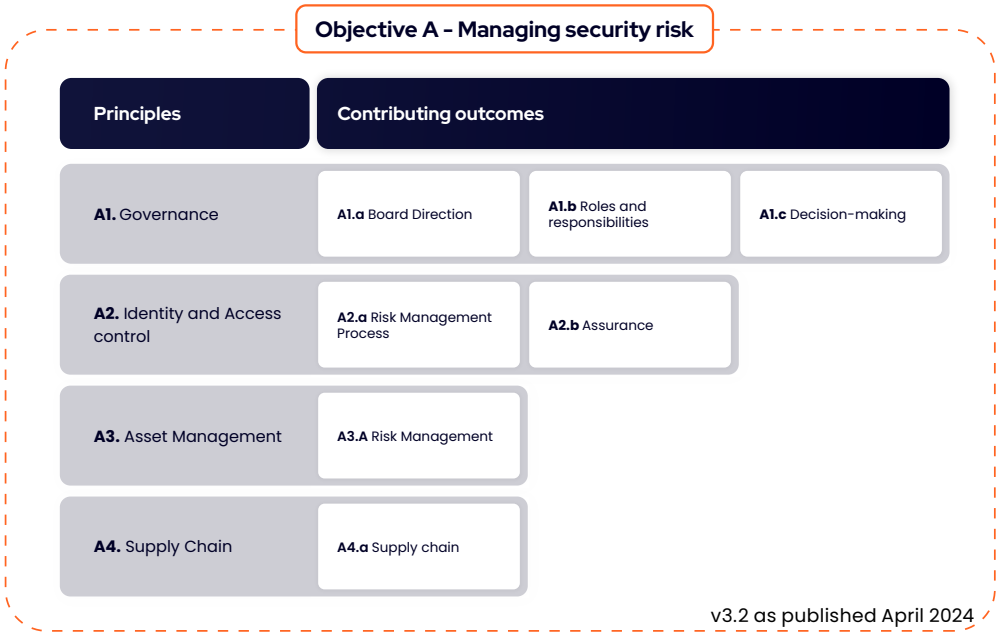
Here’s an example of everything together.



CAF objective A: Managing security risk

The CAF begins with managing security risks. And rightly so. This is the foundation of protecting your essential functions.

Objective A is all about making sure you've got the right structures, policies and processes in place to understand and control risks effectively.



Here's what you need to focus on:

A.1. Governance

First off, your organisation needs clear policies and decision-making processes that fit how you operate.

Security shouldn't feel separate. It should be baked into how you run things every day. Everyone, from leadership to your technical teams, needs to know their role in managing risks. Your communications must be crystal clear.

A.2. Risk Management

When it comes to risk, you need a plan that works for your organisation.

Don't be generic. Start by identifying what could go wrong, figure out how serious it is and tackle it. If you're dealing with things like operational technology (OT), you might need a tailored strategy.

One-size-fits-all just doesn't work here.

A.3. Asset Management

I hope this is a simple truth. You can't manage risks if you don't know what's in your environment.

That means keeping track of all the systems, tools and even people that are critical to your essential functions.

And it's not a one-and-done job. You've got to keep this updated as things change, especially for OT, which often needs extra care.

A.4. Supply Chain

Finally, don't forget about your suppliers. They're part of your ecosystem, so you need to manage risks they bring too.

This includes protecting shared data, making sure contracts include security requirements and knowing your suppliers are trustworthy. It's about keeping the whole chain secure, not just your slice of it.

CAF objective B: Protecting against cyber attacks

Let's get into the nitty-gritty of protecting your organisation against cyber-attacks.

Objective B is all about making sure you've got the right measures in place to keep essential systems and data safe.

Here's how you can tackle it, one principle at a time:

B.1. Service Protection Policies, Processes, and Procedures

Think of this as your cyber playbook. Your policies and procedures should be clear, adaptable, and updated regularly.

They need to guide your entire organisation, from leadership down, and fit seamlessly into your day-to-day operations. Don't just set them and forget them. Review them after incidents to keep improving.

B.2. Identity and Access Control

Who's got the keys to your kingdom?

Make sure you know exactly who (or what) has access to your systems and sensitive data. Limit access to only what's necessary, and regularly review permissions.

Strong verification, like multi-factor authentication, can add an extra layer of protection, especially for high-stakes access.

B.3. Data Security

Your data needs to be locked down, whether it's stored or in transit.

Protect sensitive data from unauthorised access, but don't stop there. Make sure its integrity and availability are covered too.

Think backups, encryption and even physical protections where needed. And yes, don't forget about securely wiping devices before disposal!

B.4. System Security

This is about closing as many doors to attackers as possible.

Patch your systems regularly, turn off unnecessary features, and train your staff to avoid common mistakes like falling for phishing emails.

Security isn't just about tools. It's about getting the basics right and keeping them up to date.

B.5. Resilient Networks and Systems

What happens if something goes wrong?

Build resilience into your systems so your essential functions can keep running, even under attack.

Manual workarounds, strong maintenance practices and protecting admin tools are all part of the mix. It's not just about defence. It's about bouncing back stronger.

B.6. Staff Awareness and Training

Your team is your first line of defence. And sometimes your weakest link.

Equip them with the knowledge and skills they need to spot risks and respond effectively. Tailor training to how your people actually work and focus on creating a culture where security feels like a shared responsibility.

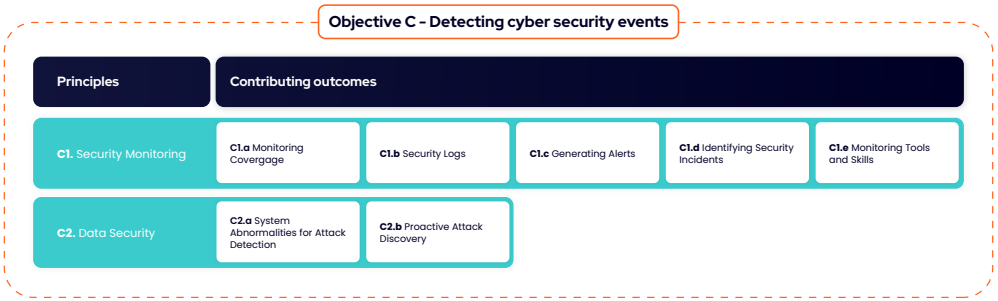
By following these principles, you're not just ticking boxes. You're building real, lasting security that works for your organisation.

Cyber attacks aren't going away, but with these steps, you'll be ready for them.

CAF objective C: Detecting cyber security events

Even the best defences won't stop everything. This is why detection is critical.

Objective C focuses on spotting cyber security events, whether they've already happened or are lurking on the horizon. This is help you can act quickly to protect your essential functions.



C.1. Security Monitoring

Think of monitoring as your eyes and ears.

It's about more than just gathering logs. it's about analysing them with the right tools and expertise to spot anything suspicious.

Regularly review your defences. New vulnerabilities and changing tech mean you can't just "set it and forget it."

Focus on what's critical: systems and assets tied to your essential functions. With strong monitoring, you'll catch problems early and be ready to respond.

Read how to go from 'not achieved' to 'achieved' for security monitoring with a managed xdr service.

C.2. Proactive Security Event Discovery

This takes detection to the next level. Instead of just reacting to known threats, you're hunting for what's unusual.

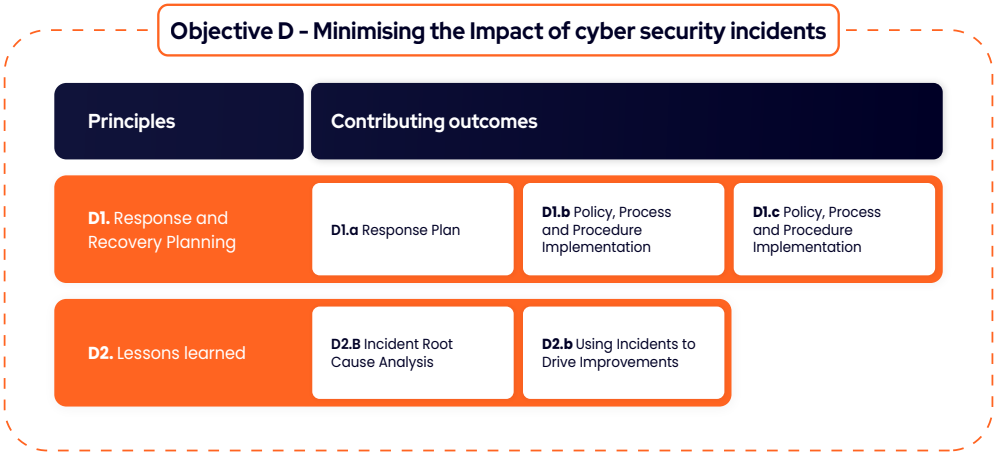
This requires a deeper understanding of your systems, normal behaviour and the creative ways attackers might try to infiltrate. It's complex. Tools like machine learning can help but it's not for beginners.

If your basic monitoring isn't rock-solid yet, start there first.

CAF Objective D: Minimising the Impact of Cyber Security Incidents

No matter how prepared you are, cybersecurity incidents will happen. Enter **Objective D.**

The focus here is all about minimising their impact on your essential functions and quickly getting things back on track.



Here's how Objective D helps you stay resilient:

D1. Response and Recovery Planning

When things go wrong, you need a solid plan to keep things running.

This means having clear, tested processes in place to respond to incidents and quickly recover if necessary.

Think of it as your business continuity safety net. Whether it's DDoS protection, power backups, critical system redundancy, or manual workarounds, make sure you've got a range of mitigation measures in place to keep essential functions intact.

Don't forget to check for any mandatory reporting requirements for cyber incidents, too.

D2. Lessons Learned

Incidents can be tough. However, they can offer you valuable learning opportunities.

After an event, take a step back and assess the root causes. It's not just about fixing the immediate issue; focus on the bigger picture.

For example, instead of just applying one missing patch, improve your patch management process to prevent future issues. Use the incident as a springboard for continuous improvement.

What makes the CAF so good?

I want to take some time to talk about what makes the CAF so effective.

It's not just a framework for the sake of having one. It's been built with a clear set of goals to help organisations like yours improve their cyber resilience and ability to respond to threats.

Here's what it's designed to do:

Help you assess cyber resilience
The CAF gives you a practical way to evaluate how well you're protecting your organisation from cyber risks.

Focus on outcomes, not tick-box exercises
It's not about just going through a list and checking boxes. The CAF keeps you focused on achieving real results, like stronger security and resilience.

Work with existing guidance and standards
If you're already using recognised cybersecurity standards or guidelines, the CAF won't replace them—it complements and works alongside them.

Identify areas for improvement
The CAF helps you spot what's working and where you need to step up your game, so you can focus on meaningful improvements.

Be universal but adaptable
The core version of the CAF is designed to work across different industries, but it's flexible enough to be tailored to specific sectors when needed.

Set realistic security goals
With the CAF, you can set achievable security targets that align with your organisation's needs or even meet regulator expectations.

Keep it simple and cost-effective
It's designed to be straightforward to use and affordable to apply, so it won't overwhelm your organisation or break the bank.

By sticking to these values, the CAF ensures that your organisation gets a practical, flexible and effective tool for managing cyber risks.

It's not just about compliance. It's about building real resilience.

A quick word on CAF profiles

You might be thinking that this already sounds like a lot, and you'd be right.

However, I must stress that you are NOT required to rate all 39 contributing outcomes as 'achieved' to successfully complete the CAF. That would take a Herculean effort on your first attempt, draining vital budget, resources and headspace.

Even the NCSC say this would be "some way beyond the bare minimum 'basic cyber hygiene' level".

This is where the concept of 'CAF profiles' come into play. Different flavours from the original vanilla. (Side note: Now I want ice cream).

CAF profiles are agreed at an individual sector level by their recognised cyber-oversight body. They will benchmark the contributing outcomes that should either be rated as 'achieved', 'partially achieved' or 'not achieved' across the principles and objectives.

The idea here is incremental improvements. Year one might dictate that 15 contributing outcomes should be 'achieved' and 15 should be 'partially achieved'. That leaves 9 'not achieved'.

Year 2 might shift to 20 being 'achieved', 15 'partially achieved' and 4 'not achieved'. And so on.

In some CAF profiles, you might find that certain contributing outcomes that are always set to 'not achieved' as they are not deemed relevant to that industry.

I will admit this is a rather crude example but hopefully illustrates the idea of how you can improve with the CAF over time.

There is also space for CAF profiles to have customised contributing outcomes and/or IGPs to better clarify meaning within their sector. This could be mean tweaking the wording slightly, or in some cases, adding completely new objectives, principles, contributing outcomes or IGPs.

You will have to check whether your industry has a sector-specific CAF profile becoming starting your assessment.

9 steps for getting started with the CAF effectively

If you're ready to start putting the CAF to work in your organisation, here's a step-by-step guide to help you get started and make the most out of the framework.

1. Check for sector-specific guidance

Before diving into the CAF, look for any sector-specific guidance that applies to your organisation.

If you're in healthcare, local government, or another sector, there may be tailored versions of the CAF or extra resources like the CAF-aligned Digital Security and Technology Principles (DSTP) for healthcare or CAF for local government.

Ensuring you have this in mind will shape how you apply the rest of the framework.

2. Understand the CAF

Take time to fully understand the CAF's objectives, principles and outcomes.

These are the building blocks of the framework and knowing why each one matters will help you apply them effectively.

These will guide you toward achieving key outcomes for cyber security and resilience, and understanding them upfront sets the foundation for everything else.

3. Interpret the principles

The CAF isn't one-size-fits-all.

After understanding the principles, you need to interpret them in the context of your organisation. Consider your size, structure, risk profile and sector to ensure you're applying the principles in a way that works best for your unique situation.

4. Set your scope

Now that you have a solid grasp of the principles and how they fit with your organisation, it's time to define your scope.

Identify the essential services and critical systems that need the most protection. This helps you focus your efforts on the areas that are most important and will guide the rest of your CAF process.

5. Get the right people involved

Identify key team members early, including IT, operations, and leadership.

Ensure everyone understands their role and how it fits into the larger goal. Use collaboration tools to keep communication open and organised, ensuring smooth progress throughout the CAF assessment.

6. Plan accordingly

Break the CAF assessment into smaller, manageable stages.

Use quieter periods to tackle big tasks and set realistic timelines. Focus on completing tasks thoroughly, and schedule regular check-ins to keep the team aligned and spot blockers early.

7. Compare practices

With your scope defined, start comparing your current practices against the CAF.

Use the guidance provided in the framework to assess how well your organisation is doing in key areas of cyber resilience. This will help you see where you stand and where you need to make improvements.

8. Identify gaps

As you compare your practices, you'll likely spot some gaps or areas that need improvement.

Prioritise these gaps based on their potential impact on your organisation's security. Not all issues are equally urgent, so focus on addressing the most critical gaps first.

9. Take action

Once you've identified your gaps, it's time to take action.

Use the CAF's guidance to start making the necessary improvements. This might involve improving IT systems, providing better staff training or addressing vulnerabilities.

Acting will help you improve your organisation's resilience and security in a meaningful way.

Wrapping up this guide to the Cyber Assessment Framework

By following these steps, you're not just ticking boxes. You're genuinely working toward improving your organisation's cybersecurity, resilience and ability to respond to attacks.

The CAF helps you take a complete, proactive approach, so your organisation is better prepared for whatever cyber challenges may come its way.