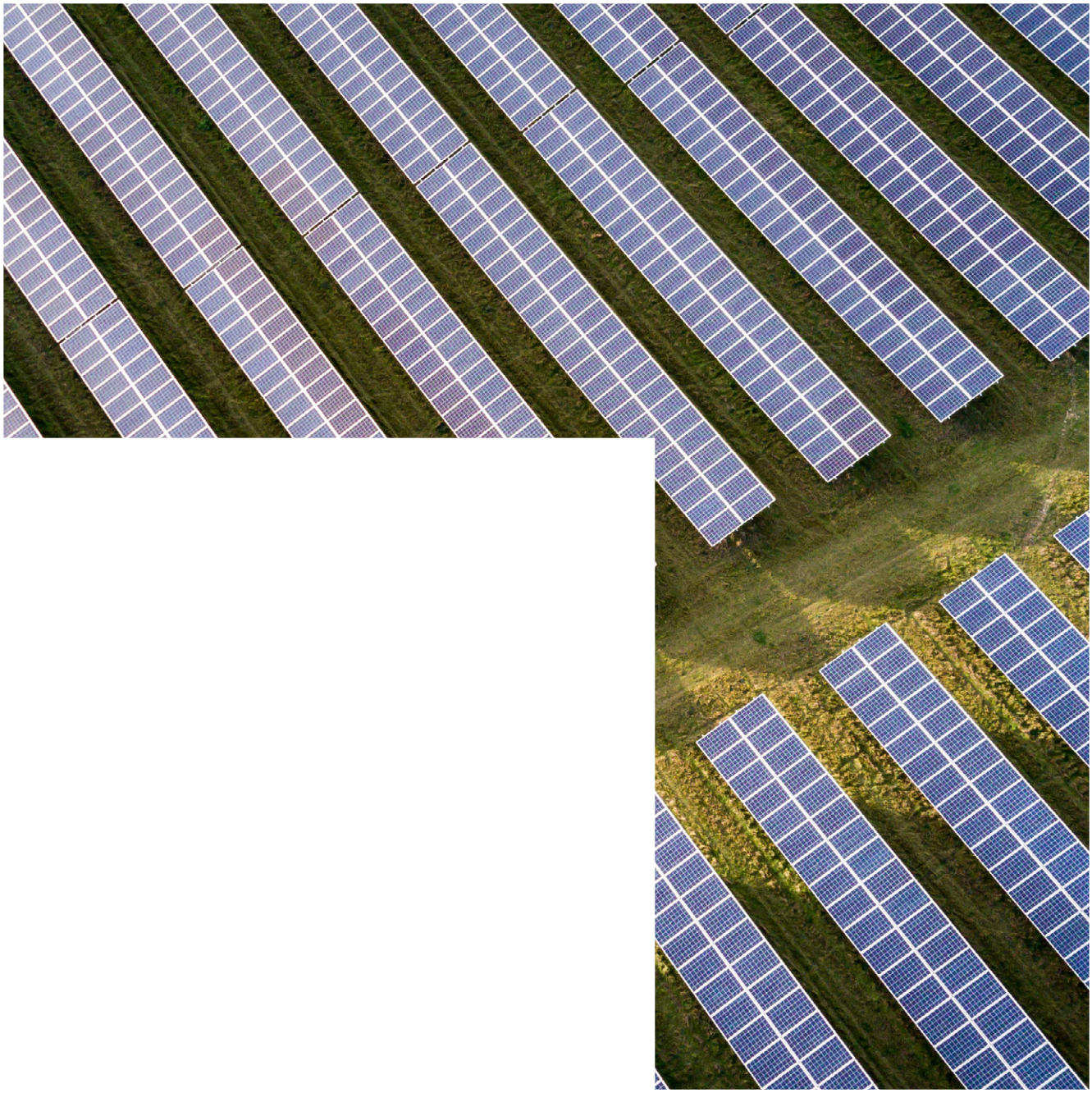


Beyond Critical National Infrastructure (CNI)

How CNI-like organisations can benefit from appropriate application of the Cyber Assessment Framework (CAF)

CGI

We all rely on our CNI; after all, that's what it means.

The good practices of its providers, suppliers and maintainers are crucial to those infrastructures being available when needed.

Contents

Authors

Dr Alex Baxendale

VP Consulting Expert (Cyber)

Alex Baxendale is CGI UK's Cyber Liaison lead for Digital Utilities

Alex re-joined the CGI Cyber Security Practice in 2006, with a particular focus on security architecture and design but also security governance.Alex has delivered security services across a broad range of industry segments within his career but has, for the past nine years, been directly supporting the utilities sector in the design, build and operation of sensitive national services.

Within the Cyber Security Practice, Alex is responsible for CGI UK's technical vision, standards, knowledge transfer, innovation strategy and technical training. He runs the UK cyber cloud innovation, mentoring and, break and learn programmes. Alex is also the cyber security liaison for all CGI Energy and Utilities opportunities in the UK.

Alex is an active participant in the support of his profession, engaging with bodies including the UK Cyber Security Council, the Digital Policy Alliance and the techUK Cyber Security group. Alex is a full founding member of the Chartered Institute of Information Security, a senior member of the Information System Security Association and Vice President (former President) of the ISC2 Thames Valley Chapter. Alex currently holds CISSP, ITPC and SABSA

Foundation status and is a Senior Security and Information Risk Advisor under the NCSC Certified Professional (CCP) scheme.

Rich Hampshire

VP Consulting Expert (Utilities)

Rich Hampshire is CGI UK's lead for Digital Utilities

Rich joined CGI in 2007 working across its 'digital' utilities offerings. He has over 30 years' experience in the utilities sector, covering areas including competitive energy markets, energy services and energy retail, smart meter and smart grid strategy.

He is active in the leadership of a number of industry associations, including being the chair of the techUK's Smart Energy and Utilities Board and a member of the Smart Infrastructure and Systems Advisory Council.

Rich is a regular speaker at utility events and has authored numerous papers, which include the Beyond Smart – generating the demand-side flexibility opportunity for British energy white paper and the ever popular Energy Flexibility For Dummies book. Rich is also the driving force behind CGI's research on energy flexibility in collaboration with Utility Week.

Rich is a professional engineer by background and has spent his career working with organisations to implement transformation.

Executive summary

We all rely on our CNI; after all, that's what it means. The good practices of its providers, suppliers and maintainers are crucial to those infrastructures being available when needed. It should be no surprise to say that this is a highly regulated space. Here in Europe, this typically means alignment to the EU Network and Information Systems Directive (NIS-D), enforced in the UK via the UK Network and Information Systems Regulations (NIS-R) 2018.

This regulation requires providers to follow the Information Commissioner's Office (ICO) guidance as the competent authority. At present, this means following the Cyber Assessment Framework (CAF) as published by the National Cyber Security Centre (NCSC). For organisations that fall within the scope of NIS-R, the CAF represents a statement of expectation about conducting operations within essential services.

CGI has considerable experience leveraging this framework in support of our clients. It is this experience that has led us to understand how the CAF, when applied appropriately, provides a useful toolkit for 'CNI-like' organisations that are outside of the pure CNI umbrella. For these CNI-like organisations to benefit from applying the CAF, its principles need to be applied sensibly, cognisant of the organisation's specific needs and business priorities and in support of their established tooling and governance frameworks.

If you are interested in how we reached this conclusion and would like to understand whether your organisationcould benefit too, please read on.

Cyber assurance in the CNI space

According to the National Protective Security Authority (NPSA) 'National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends.' There are 13 national infrastructure sectors in the UK, including energy and water, with each sector being overseen by one or more lead government departments (competent authorities).

Of those national infrastructures, some are deemed 'critical'. The UK's official definition is:

Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

1. Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts
2. Significant impact on national security, national defence, or the functioning of the state

It's a concept subject to some subjectivity. Whether any specific service is CNI will depend on the lead government department's determination, guided by the NCSC and the Cabinet Office.

Critically, if you are an operator of services in one of the 13 national infrastructure sectors, you need to be cognisant of the UK Network and Information Systems Regulations 2018 (NIS-R). This regulation was transposed from the EU Network and Information Systems Directive (NIS-D), which provides legal measures to boost the overall level of cyber security in the EU and is aimed specifically at key systems.

NIS-R defines:

- The National Framework (Part 2),
- Operators of 'essential services' (Part 3) and their responsibilities,
- Digital Services (Part 4),
- Enforcement and penalties (Part 5), and
- Designated Competent Authorities (Schedule 1) acting as leads.

Importantly, this requires a person to notify the designated competent authority when the essential service they provide:

- relies on network and information systems, and
- meets a threshold requirement documented in Schedule 2 of said regulation for each sub-sector (including electricity, gas, oil and water).

The competent authority may designate that person as an operator of an essential service, whether they have notified the competent authority or not! Currently, the Secretary of State for Energy Security and Net Zero, acting jointly with the Gas and Electricity Markets Authority (GEMA), is the designated competent authority for electricity, gas and oil.

NIS-R obligations

NIS-R sets out the security duties of operators of essential services. These are:

1. Take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which essential services rely

2. Take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service with a view to ensuring the continuity of those services

The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed. This will provide a re-enforcement of the core mantras of information and cyber security, namely, manage risk and implement proportionate controls to safeguard your assets.

Critically, it goes on to say, "…Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) and (2)". It is necessary to respond to the supplied guidance, publicly published or not, as provided by the competent authority.

CNI-like

However, there are many services and assets that are not formally deemed critical but interface with critical systems or have owner assessments that seem very closely aligned to this definition. Such services and assets are described as being ‘CNI-like’. Assessment against the associated standards and assurance frameworks offers real value. You may not need to be certified, but alignment demonstrates commitment and effective risk management.

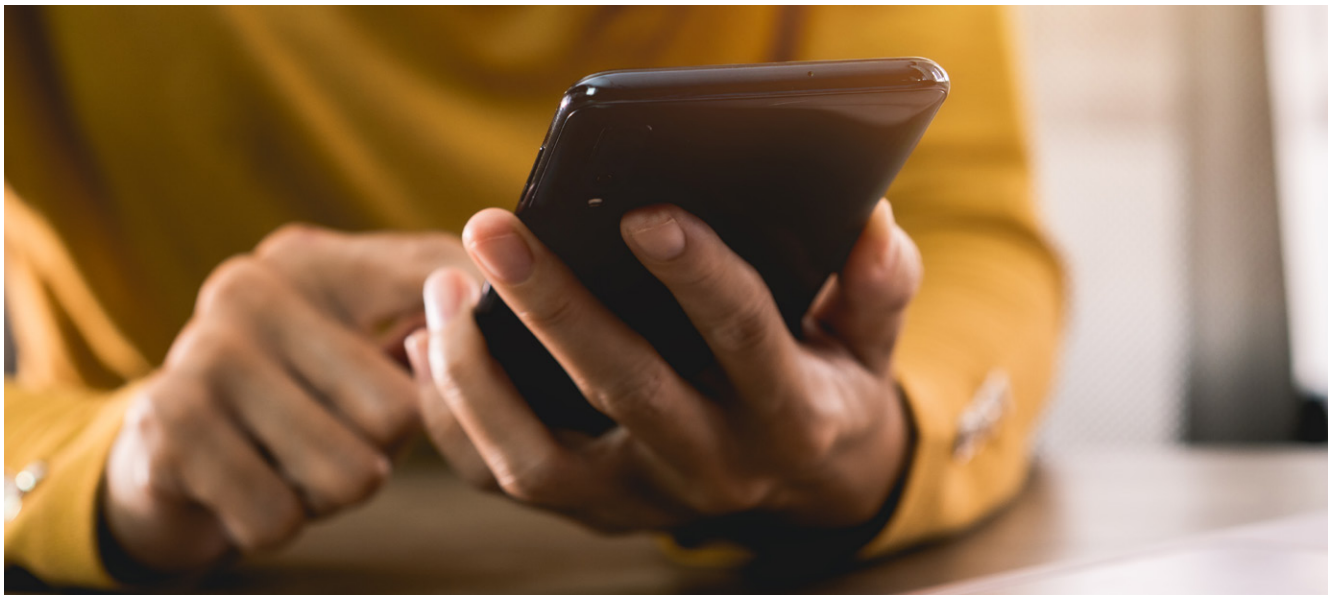
Ask yourself these questions if you think you are ‘CNI-like’:

- Is your service critical for your operations?
- Would its compromise have a significant impact on your customers, suppliers, or other stakeholders?
- Would the impact be far-reaching in terms of societal effects?
- Do you think your service would be of interest to high capability threat actors, such as organised crime and foreign governments?
- Do you rely on Operational Technologies (OT)?
- Does it seem aligned to the UKs’ ‘critical’ infrastructure definition?

If the answer to any of these is ‘yes’, you should consider your service to be ‘CNI-like’.

You may not need to be certified, but alignment demonstrates commitment and effective risk management

What's out there?



Having elevated risk will require either a high risk tolerance or investment in appropriate and proportionate controls to mitigate and manage that risk. You can always take standard commercial security frameworks like ISO27001 and ISO27005 to create a baseline to build from to manage the risks and seek independent assurance. This has been done effectively through certification and the likes of SOC2. SOC2 is an audit procedure that ensures service providers securely manage the data they hold on behalf of their customers. Here in the UK, SOC2 has been growing in popularity. It provides attestation and is suited to targeting a specific service or capability rather than a whole organisation, and fits with critical services. Many now adopt the NIST Cyber Security Framework (CSF) and align it to the higher tiers for better assurance services. For example, an organisation or service owner proactively instigating cyber security measures adaptively. This is supported via the SP-800 series of cyber-related guidance documents. While commendable and in many cases necessary, this approach on its own arguably fails to leverage the advantage of those experiences of others captured and enshrined in higher assurance standards.

In the UK, the NCSC has developed the Cyber Assessment Framework (CAF) to support operators of essential services, which, according to the NCSC, "…provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible." The NCSC is the UK's national technical authority on cyber security, and your competent authority will refer out to their guidance. The good news is that NCSC has been moving on a journey towards ever further publication of such guidance into the public domain, and the CAF is no exception.

The CAF has been designed as a framework for assessing resilience against NCSC cyber security and resilience principles. It is outcome-focused and compatible with other cyber security standards, such as the ISO 27000 series and NIST 800 series. It is also modular, supporting generic and sector-specific guidance to be followed and contributing outcomes in terms of profiles.

How the CAF works

We operate services on behalf of clients across all of the 13 national infrastructure sectors. Some are formal CNI, and many are seen as highly sensitive and businesscritical by our clients. Within utilities, this is especially true, and many such services may be deemed ‘CNI-like’ or touching on CNI.

On one of CGI’s larger programmes, our client’s services have not been designated as CNI. However, there are many aspects of the service that are CNI-like; with high availability requirements, high-value assets, privacy implications and elements of interest to high threat actors. It would not surprise you to hear that the controls applied to this service are risk-aligned and extensive. They include all of the standard capabilities you would expect for CNI, with the service being subject to ISO 27001 certification and SOC2 audit. Alongside this, we compared our service against the guidance available in the CAF to understand alignment and see if there are any obvious areas for improvement missed, leveraging the CAFs encapsulation of the CNI experience.

Applying the CAF

NCSC guidance can be found on their website. We summarise this in the following to set the scene.

The CAF assesses alignment against each of its security and resilience principles and objectives:

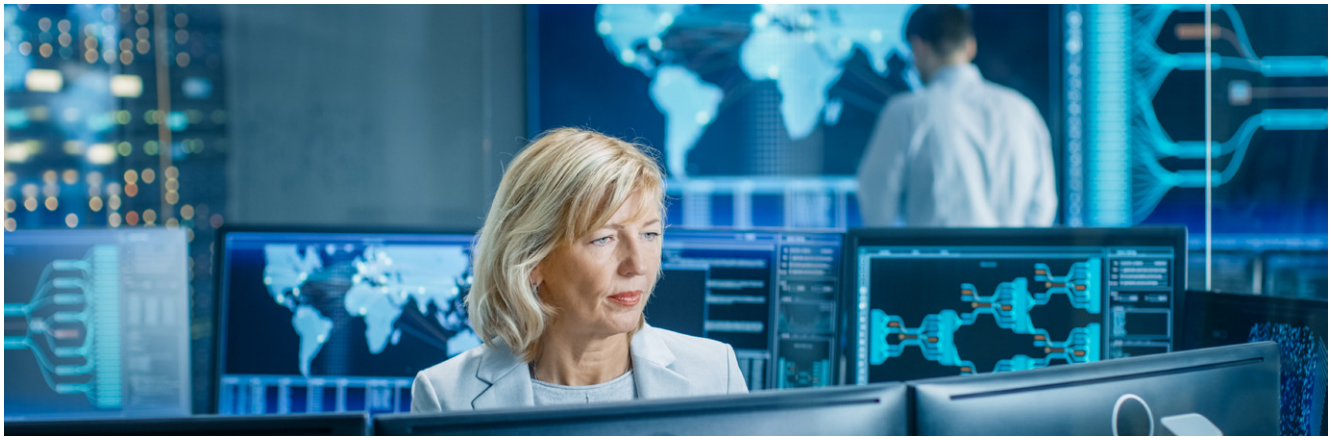
A. Managing security risk – CGI assess the risk

B. Protecting against cyber attack – CGI protect the business

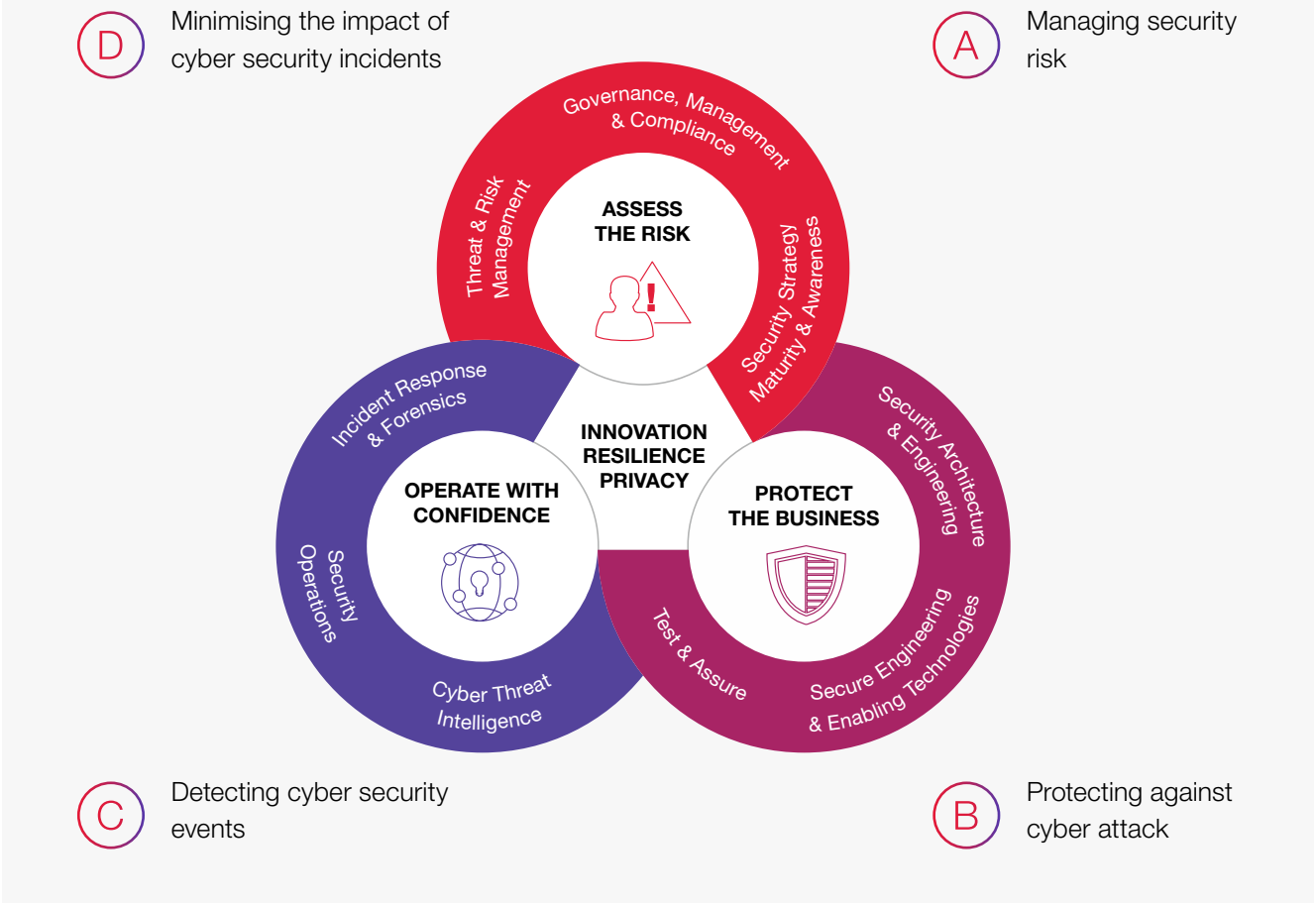
C. Detecting cyber security events – CGI operate with confidence – security operations

D. Minimising the impact of cyber security incidents – CGI operate with confidence – incidence response

Compliance against a set of desired outcomes are broken down into a set of Indicators of Good Practice (IGPs). This hierarchical approach allows the break down of a complex assessment into manageable chunks and provides flexibility in application. Any experienced cyber security professional should feel comfortable with these. The high-level objectives cover the areas anyone familiar with ISO27001 and similar frameworks will recognise and align well with how CGI supports our clients.



Cyber Security Wheel



There are 39 individual assessments associated with the CAF's desired outcomes, each with its own IGP set. Helpfully, the CAF details the contributing outcomes and associated IGPs into a set of IGP tables, one table per contributing outcome, making this very suitable to spreadsheet tracking, analysis and reporting. Using a tab for each table and collating into a mastersheet to provide one-to-many reporting dashboards with graphs and tables works well.

When it comes to CAF compliance, you assess alignment against each of the IGPs based on 'achieved', 'partially achieved' or 'not achieved', usefully aligned to a RAG status. These IGPs include both good behaviours to be exhibited and bad behaviours to be avoided. We illustrate this in the following graphic for Risk Management Principle A.2, with a made-up non-compliance.

Principle A2	**Risk management** The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.	
A2.a	**Risk management process** Your organisation has effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services and communicating associated activities.	
Assessment:	**Not achieved**	Select response based on the following indicators.
Justification and further comments:	State reason for assessment with reference to the indicators below.	
Indicators	Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve - await funding for lots of remediation activity. You perform threat analysis and understand how generic threats apply to your organisation - this is weaker and reliant on the flow of vulnerability and threat information. Otherwise, the majority of the partially and achieved sections are completed.	
Not achieved - at least one of the following statements is true.	**Partially achieved** - all of the following statements are true.	**Achieved** - all of the following statements are true.
Risk assessments are not based on a clearly defined set of threat assumptions Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. Risk assessments for critical systems are a 'one-off' activity (or not done at all). The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service. The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security.	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed. Your approach to risk is focused on the possibility of disruption to your essential service, leading to a detailed understanding of how such disruption might arise as a consequence of possible attacker actions and the security properties of your networks and information systems. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential service and your sector.

Good behaviour must be met with no bad behaviours exhibited to achieve a pass. For example, one bad behaviour would normally be sufficient to justify an assessment of 'Not Achieved' for its associated desired outcome. In the above example, failure to ensure that a risk assessment is easy to understand, would still result in a fail, even if you meet all of the partial criteria and most of the achieved criteria.

For cyber security people, this concept will be well understood and forms part of the cyber mindset. Experience proves the value of identifying and addressing bad behaviours, as it is often the bad behaviours that result in vulnerability and risks being realised. For example, when you get a penetration testing report, you can fix the issues identified, or you can assess the underlying root cause and fix that. Experience indicates that the root cause will often be bad behaviour, and fixing the root cause is invariably the best long-term solution.

Can your controls be deactivated, bypassed or even used against you? In the testing world, it is analogous to move from standard use case testing to consider misuse cases and, dare we say it, ethical hacking. It is a good example of the additional value that can be derived from applying the CAF.

Perhaps ironically, this is where most parties using the CAF for the first-time struggle. They generally score quite well against the desired 'good' behaviours but relatively poorly against the bad behaviours. This probably reflects the inherent bias of many other assurance and evaluation schemes that tend to focus on the sorts of controls you should be implementing but less so on what you should not be doing. Arguably two sides of the same coin, but our experience suggests not.

We also find that most parties conducting their own analysis generate many 'partially achieved' amber evaluations. There is a tendency to put amber when you do something relevant and to discount poor behaviours. The nature of the criteria is to some extent subjective. Any in-house assessment may invoke favourable, potentially unconscious, bias. "…well, I think my risk assessment is easy to understand, so a tick on that one." Never mind what the decision-makers think of it.

For cyber security people, this concept will be well understood and forms part of the cyber mindset

CAF techniques

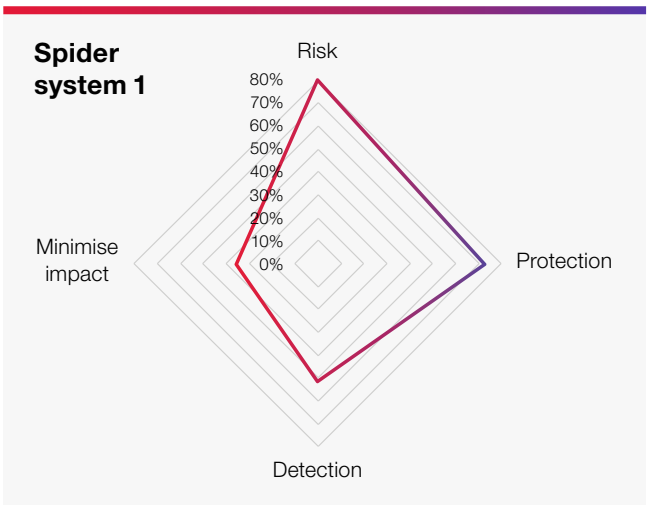
The CAF is a flexible tool that can be used to consider the health of a specific service at any given point in time, over time and/or relative to other systems. Patterns of non-compliance, including sector or service-based, will undoubtedly arise, and comparisons between organisations and systems might provide some true insight into the relative success of individual parties and actions plans over time. While a designated competent authority can use such techniques for inter-organisation and service comparison, there is nothing stopping individual organisations doing the same across consenting parties. This can either be for distinct services, managed service providers or system integrators.

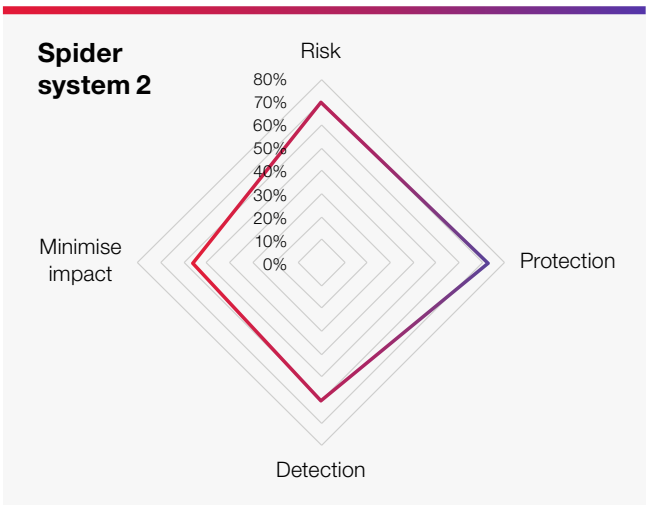
Weightings could also be overlaid to compliance against specific criteria based on alignment to organisational policy, architectural principles, perceived threats or between achieved and partially achieved. However, these would need to be consistently applied for meaningful comparisons and could potentially be misused to bend the results towards what you want to see.

It should be stressed that the CAF is not intended to be a tick box checklist, albeit aspects of it can feel like that. It is meant to be a framework to help parties make an informed judgement about their current security posture and how that can be improved to align to good practice for CNI-like organisations. There is an aspect of 'pick and mix' in the selection of applicable IGPs. This will often form part of a profile for a sector or service, determined by the competent authority.

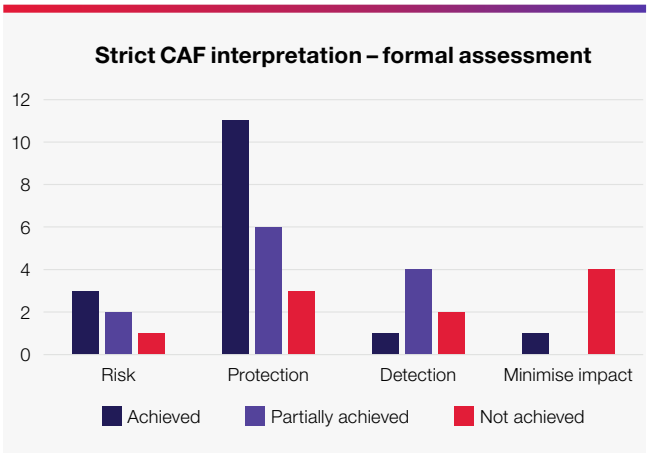
If you are CNI-like, you have a lot more freedom to define your profile and levels of compliance. While it's hard to defend a bad behaviour, our experience shows that where a hard formula says non-compliance results in failure, this could seriously distort the overall picture of the organisation or system under assessment when prioritising remedial action. This can lead to wild fluctuations in compliance patterns over time or between systems, which undermine the comparative analysis.

CAF IGP achievements

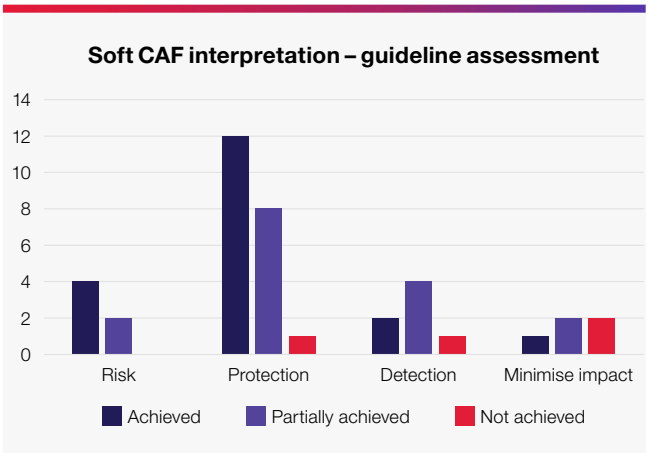




Strict CAF interpretation – formal assessment



Soft CAF interpretation – guideline assessment



For CNI-like scenarios, we have often found it useful to conduct both a pure compliance assessment, as if you were a scheme auditor, and a revised assessment with a softer interpretation of the rules, by weighting responses based on agreed criteria. The former drives the long-term vision and helps management understand just how far they are from full alignment. The latter drives your immediate priorities because understanding your posture and its limitations is just the starting point to getting to where you want to be; a better place. Also, it requires an action plan. However, the very nature of CAF IGPs is helpful when it comes to defining those actions. For instance, where "…

Monitoring staff have some investigative skills and a basic understanding of the data they need to work with" (which would be partially achieved against Principle C1.e) but then fail to meet the statement "...Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them" - the action item is obvious. You would need to enhance staff training and awareness, providing easy access to tools and information to keep on top of such things. This represents a true value add for the CAF.

Beyond the CAF

A CAF assessment should not be a standalone exercise. It is merely a mechanism for enhancing the understanding of your risks and controls. Leveraging and integrating its findings into your current governance control mechanisms, especially your risk management processes, ensures that it becomes part of your standard policies and processes.

The existence of a 'partially achieved' or 'not achieved' rating against an IGP implies that there is some risk you are not adequately countering. Perhaps one you have not even identified. The existence of a bad behaviour probably means that some of your extant controls are deficient or not effective. Back to our analogy, having a risk assessment is not effective if the decision-makers cannot understand what it's telling them or cannot see the 'wood for the trees'.

Understanding the cost, time, and effort involved in implementing any controls or measures is critical to any investment priorities decision. Also, there are invariably many different ways of achieving any compliance objective. Making your risk assessment more understandable to the executives may be a matter of report presentation, perhaps some new dashboard or summary. However, it may involve using new visualisation tools or adopting a more enterprise-grade risk management system.

Indeed, the CAF, like any standard, can be built into many enterprise-grade risk management tools to provide a more industrialised and dynamic assessment, monitoring and reporting tool. Such tools can be used to develop Key Performance Indicators associated with alignment to a good or bad behaviour. They can then be used to provide evidence of compliance to support future audit and allow for a timelier response to any implementation failure. When integrated with data analysis tools like ELK stack or SIEM monitoring tools, this can provide an ongoing picture of compliance and effective governance.

The CAF is also a useful tool to model the before and after of any action plan.

It illustrates the benefits derived from any investment in action and is relatively straight forward to implement within a spreadsheet model.

Conclusion and recommended action

For organisations that fall under the CNI in terms of NIS-R, as moderated by your competent authority profile, the CAF represents a statement of expectation about how you conduct operations within your essential services. You need to baseline your current compliance and identify areas of weakness. Deficiencies need to be addressed, and plans agreed with your competent authority. Priorities should be driven based on good risk management. Like cyber security more generally, this is an ongoing process of improvement and adaptation as your service, the threat environment, and the CAF itself evolves. Therefore, this is an iterative journey towards enhanced maturity.

For CNI-like organisations, it represents another useful tool in your armoury. It can be used to compare your posture with a similar type of organisation and contains a suite of good practice statements that provide real insight into areas of potential deficiency and action areas to improve. Its use of 'bad behaviours' adds a do's and don't's dimension, which has real value. The nature of its statements makes them well suited to defining action points.

CAF is suitable for integration into and alignment with governance standards. Some flexibility in its interpretation should be applied to ensure it supports rather than distorts your cyber investments.

In practice, you will need to identify action points and devise a plan of measures necessary to deliver these to form part of your overall investment approach. After all, this is where the true complexity lies.

CGI and the CAF

Our CAF experience derives from a combination of CGI cyber consulting services business and our operations as a prime systems integrator and service provider for organisations across the 13 national infrastructure sectors, including utilities. That experience covers the entire operations lifecycle and all four CAF objectives.

CGI provides independent pre-assessments of compliance. We support organisations in defining, delivering and implementing resultant action plans, introducing industrialised and automated services to facilitate ongoing management. We provide holistic intelligence-based input to allow an organisation to compare against their peers.

As long as the CAF is applied sensibly, it remains cognisant of an organisation's specific needs and business priorities and supports established tooling and governance frameworks, we believe the CAF provides a powerful toolkit for organisations outside of the pure CNI umbrella.

References

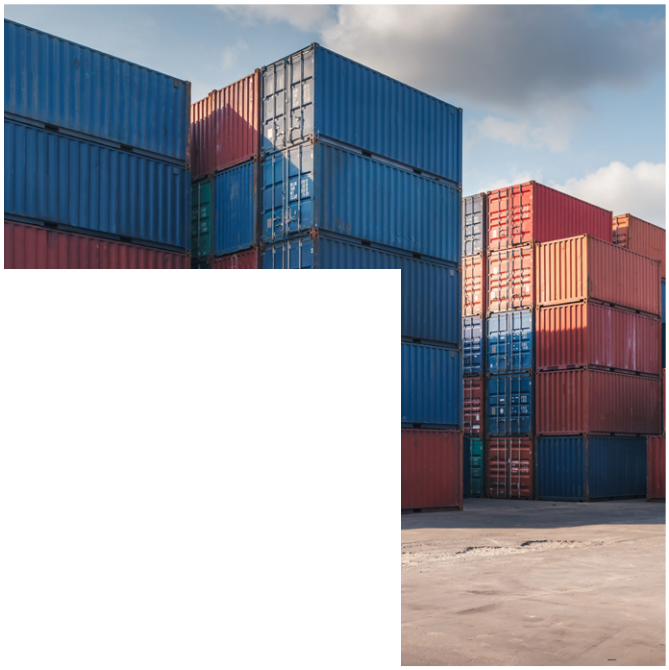
EU Network and Information Systems (NIS-D) Directive, enforced in the UK via the UK Network and Information Systems Regulations 2018. The Network and Information Systems Regulations 2018 (legislation.gov.uk)
legislation.gov.uk/uksi/2018/506/made

Critical National Infrastructure | NPSA
npsa.gov.uk/critical-national-infrastructure-0

National Cyber Security Centre
ncsc.gov.uk/section/advice-guidance/all-topics

NCSC CAF guidance
ncsc.gov.uk/collection/caf

NCSC CAF guidance, risk management
ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a2-risk-management



About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information, visit cgi.com/uk or email us at enquiry.UK@cgi.com