FACTSHEET

MEET THE CAF'S OBJECTIVES WITH LITTLEFISH

littlefish
CYBER SECURITY SERVICES

Welcome to Littlefish

Where cyber security is done a little differently...

Alongside our technical excellence and proactive threat-monitoring activities, we believe that cyber security should be delivered in a personalised, people-centric, and authentic way.

Our approach is always collaborative and agile; we're passionate about providing security solutions that not only protect your organisation but enhance your business performance and add tangible value too.

Used by Critical National Infrastructure (CNI) such as electricity, water, oil, and gas organisations, as well as NHS Digital, which recently assured all their services against the framework, the National Cyber Security Centre (NCSC)'s Cyber Assessment Framework (CAF) is fast becoming the predominant standard for all sorts of organisations as a measure of best practice for cyber security.

Here at Littlefish, we have the expertise you need to provide the guidance, planning, and protection to help you meet and keep-to CAF's objectives – with all services being carefully tailored to your risk profile and organisational needs.

The Cyber Assessment Framework

An overview

The CAF was developed by the NCSC to help organisations manage cyber risk by meeting the following set of requirements:

- To provide a suitable framework to assist in carrying out cyber resilience assessments
- To maintain the outcome-focused approach of the NCSC cyber security and resilience principles and discourage assessments being carried out as tick-box exercises
- To be compatible with the use of appropriate existing cyber security guidance and standards
- To enable the identification of effective cyber security and resilience improvement activities
- To exist in a common core version which is sector-agnostic
- To be extensible to accommodate sector-specific elements as may be required
- To enable the setting of meaningful target security levels for organisations to achieve, possibly reflecting a regulator view of appropriate and proportionate security
- To be as straightforward and cost-effective to apply as possible

At Littlefish, our team of cyber security specialists can help your organisation meet the CAF's obligations by implementing powerful and robust levels of cyber security and resilience, drawing across our wide range of cyber security services. These include:

- UK-based cyber security operations centre (CSOC)
- Managed Detection and Response (MDR)
- Managed eXtended Detection and Response (XDR)
- Virtual Chief Information Security Officer (vCISO)
- Vulnerability management
- Cyber assessment
- Managed Microsoft Sentinel
- Cyber consulting

Sterling

"Information security was becoming a bigger and bigger concern for the company, with pharmaceuticals being a highly regulated industry. For us, data security is paramount and cannot be underestimated – we needed a partner we could trust, one that could come in and hit the ground running and that was Littlefish."

Paul Southam
CIO, Sterling Pharma Solutions

Service Description

Designed to offer a comprehensive approach for all types of organisations to manage cyber security risk, the CAF is a flexible and adaptable framework that businesses can use to measure their own cyber resilience against. Meeting the CAF's obligations also lets your customers, suppliers, and employees know that you take your cyber security responsibilities seriously.

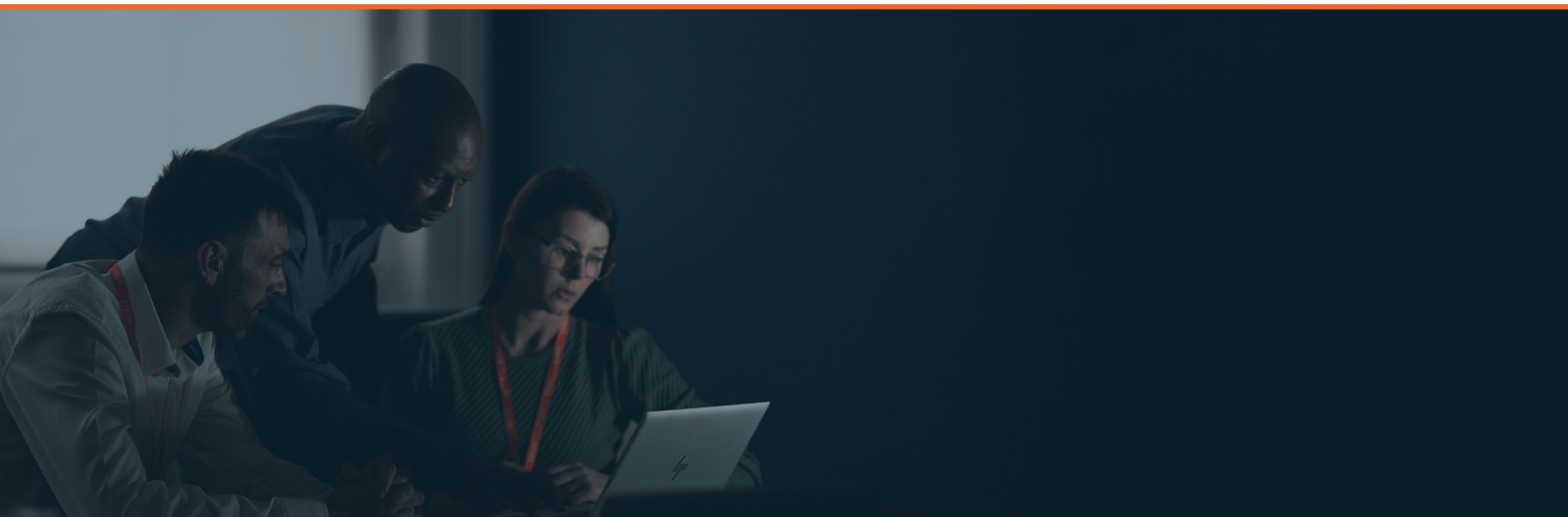
Utilising Littlefish's managed cyber security services and working alongside our information security specialists, we can ensure that your organisation understands, assesses, and systematically manages security risks following CAF's four objectives (and corresponding fourteen underlying principles).

Objective A: Manage security risk

- Putting in place policies and processes to govern your organisation's approach to the security of network and information systems.
- Identifying, assessing, and understanding the security risks affecting your organisation and establishing an overall organisational approach to risk management.
- Determining and understanding all systems and/or services required to maintain or support your organisation's essential functions.
- Understanding and managing your specific security risks tied to dependence on external suppliers.
- Assisting with establishing governance processes so that security management is considered at board level with clearly articulated roles and responsibilities and overall accountability for decision making.

Objective B: Protect against cyber attacks

- Define and communicate appropriate organisational policies and processes to secure systems and data that support the operation of essential functions.
- Understand, document, and control access to networks and information systems that support essential functions.
- Protect stored or electronically transmitted data from actions that may negatively impact essential, value-making functions.
- Protect critical network and information systems and technology from cyber-attacks and threats.
- Build resilience against cyber-attacks and become cyber mature.
- Appropriately support and educate staff to ensure they understand and contribute to the cyber security of essential functions.



littlefish
CYBER SECURITY SERVICES

Objective C: Detect cyber security events

Drawing on Littlefish's MDR, XDR, and managed Sentinel services, which offer round-the-clock, 24/7 advanced cyber threat monitoring, rapid incident response, and intelligent detection tools, we can ensure your organisation has the ability to:

Monitor systems and detect potential security problems and track the effectiveness of existing security measures.

Detect anomalous events in relevant networks and information systems and rapidly respond to contain cyber threats.

Objective D: Minimise the impact of incidents

With Littlefish's cyber consulting service and innovative critical hour framework (CHF) approach, we offer organisations the chance to identify different risk scenarios and prepare for them extensively,.e.g. by undertaking tabletop exercises to evaluate whether your incident response plan works effectively. Following the CAf's guidance, Littlefish is on-hand to:

Put suitable incident management and mitigation processes in place, including undertaking tabletop exercises with key stakeholders and setting in place a critical hour framework (see on next page).

Help your organisation learn from any prior incidents and implement lessons and improvements to boost the resilience of essential functions.

Tabletop exercises

A cyber crisis tabletop exercise helps organisations to identify different risk scenarios and prepare for them. Littlefish can host this activity at your organisation to evaluate whether the incident response plan currently in place works effectively in the event a cyber-attack does occur.

The exercise considers one or various simulated scenarios that could negatively impact your organisation and involves both internal and external stakeholders.

Throughout, we'll analyse the crisis management capabilities of your organisation and make recommendations for change.

Critical hour framework

As an integral part of the alert response processes, Littlefish will work with the customer's key stakeholders to develop a critical hour framework (CHF). The primary aim of the CHF is to provide a clearly defined playbook of actions to enable rapid and decisive action to be taken against an attacker to stop, prevent, and minimise malicious activities.

These actions are designed to be undertaken within the first hour of detection and qualifying alert being received. The CHF has proven to be successful in containing and minimising the impact of being targeted by skilled, persistent, motivated, and well-resourced attackers.

national gas

"This is why we partnered with Littlefish, a managed IT and cyber services provider that is nimble and understands that our diverse structure means diverse solutions. We look forward to building this partnership over the coming months and years."

Richard Murphy
CIO, National Gas

littlefish
CYBER SECURITY SERVICES

PROTECT YOUR BUSINESS, PROTECT YOUR VALUE

Security and Assurance

Littlefish are an ISO9001 and ISO27001 certified organisation (copy of certificates available on request). We are accredited to Cyber Essentials and Cyber Essentials Plus.

ISO 27001 ISOQAR REGISTERED alcumus.com
ISO 9001 ISOQAR REGISTERED alcumus.com
ISO 14001 ISOQAR REGISTERED alcumus.com
CREST | SOC

To find out more about how Littlefish can help protect your business:

Get in touch
info@littlefish.co.uk
0344 848 4440