CrowdStrike Solutions

CROWDSTRIKE

White Paper

The Cyber Assessment Framework (CAF)

Supporting security requirements to protect UK public sector organisations

Executive Summary

The contemporary adversary has emerged as an efficient, effective, elusive and evasive global threat.

In the current era marked by an escalation in cyberattacks and an augmentation of their sophistication, the threats facing the United Kingdom (U.K.) present a significant risk. To help address these threats, the National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF). The NCSC CAF carries significant weight for organisations operating within the U.K., encompassing not only those within the public sector but those delivering or supporting Critical National Infrastructure (CNI). The framework delivers a structured and methodical approach for scrutinising an organisation's cybersecurity measures and highlighting areas requiring improvement. The framework is also critically important for organisations subject to Network and Information Systems (NIS) Regulations, which require organisations to implement appropriate measures to manage cyber-related risks. Furthermore, the NCSC CAF serves as a practical tool for organisations entrusted with managing cyber risks to public safety, such as those in the healthcare or transport sectors. By following the guidance stipulated by the NCSC CAF, organisations can bolster their resilience to cyber threats, optimally safeguarding the essential services they provide to the public.

The NCSC CAF was devised in light of the growing need for a consistent and effective approach toward cybersecurity risk management in the public sector. It was also designed to support the U.K. Government Cyber Security Strategy 2022-2030, which sets forth objectives to assist U.K. organisations in gaining a clear understanding of their cybersecurity posture and safeguarding essential functions from the latest cybersecurity threats.

The Cabinet Office's Government Security Group (GSG) launched GovAssure in 2023, which makes public sector organisations — and some arms-length management organisations (ALMOs) — subject to annual assessment against the CAF, supporting standardisation and the drive toward the then NCSC Chief Executive Ciaran Martin's goal of: "Making the U.K. the safest place to live and do business online."

As the need for robust cybersecurity measures continues to intensify, organisations are seeking reliable solutions to safeguard against the most advanced threats that go beyond the traditional **detection and response** capabilities. As a worldwide leader providing cloud-based cybersecurity and threat intelligence solutions, CrowdStrike has established a prominent presence in the industry. The CrowdStrike Falcon® platform is renowned for its advanced endpoint protection, threat intelligence and managed threat hunting services, having been designed to ensure principles such as secure by design and privacy by design have been incorporated to address the ever-evolving security requirements of organisations. The Falcon platform enables organisations to defend against sophisticated cyber threats with increased efficacy.

CrowdStrike's unwavering commitment to constant innovation and relentless customer success has earned it a position as a trusted provider of cloud-delivered security solutions. Its advanced technology and expertise have equipped U.K. public sector organisations with adversarial situational awareness of the threats facing them. By leveraging CrowdStrike's solutions, U.K. public sector organisations have been able to stay ahead of the rapidly evolving threat landscape and defend against sophisticated cyberattacks. CrowdStrike's dedication to innovation and customer success is reflected in its ability to deliver effective security solutions that meet the needs of modern organisations.

Government organisations are routinely and relentlessly targeted: of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. This upward trend shows no signs of abating.

U.K. Government Cyber Security Strategy 2022-2030

Background

As a component of the EU Cybersecurity Strategy, led by the European Union Agency for Cybersecurity (ENISA), the European Commission proposed the EU NIS Directive in 2016. The NCSC subsequently released the CAF in 2018 to support organisations that must comply with the EU NIS regulations.

The NIS Directive aims to achieve three main objectives:

- First, it requires EU member states to possess certain national cybersecurity capabilities. For instance, they must have a national computer security incident response team (CSIRT) and engage in cyber exercises.
- Second, the directive calls for cross-border collaboration between EU countries via initiatives such as the operational EU CSIRT network and the strategic NIS cooperation group.
- Finally, the NIS Directive demands that EU member states supervise the cybersecurity of critical market operators within their borders. This includes ex-ante supervision in critical sectors (such as energy, transport, water, health, digital infrastructure and finance) and ex-post supervision for critical digital service providers (like online marketplaces, cloud services and online search engines).

Member states create their own frameworks to align with the NIS Directive, but the U.K. is no longer part of the EU. Nevertheless, the NIS regulations still apply to cross-border collaboration and continued alignment to the NCSC, and the NCSC CAF provides essential components for developing and maintaining a robust cybersecurity posture.

Scope of the NCSC CAF

The NCSC CAF serves as a comprehensive reference model that enables organisations in establishing, maintaining and enhancing their cybersecurity posture. Other frameworks and guidance exist — such as those provided by the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), MITRE ATT&CK®, the SANS Institute, and the OWASP Foundation — and the NCSC CAF shares several similarities, as they follow the core principles of cybersecurity best practices.

The NCSC CAF has gained increased recognition and has emerged as a primary reference for numerous organisations across the U.K., and it has also become a source of reference for organisations and bodies that are responsible for:

- Safeguarding and maintaining the CNI of the U.K.
- Adhering to the NIS Regulations
- Managing cyber-related risks to public safety within the U.K.

** The information provided herein does not and is not intended to constitute legal advice; rather, all information, content, and materials available herein are for general informational purposes only. Information herein may not constitute the most up-to-date legal or other information. Readers of this content should contact their legal counsel to obtain advice with respect to their regulatory compliance obligations and compliance programs.*

We are committed to ensuring the UK continues to be a leading global cyber nation, which is why we have supported the development of the Cyber Assessment Framework to improve the security of our most critical information systems.

Lindy Cameron, CEO
National Cyber Security Centre

Summary of the CAF Requirements

The CAF is a vital component of public sector organisations' cybersecurity risk management strategies. Aligned with the U.K. Government Cyber Security Strategy 2022-2030, the CAF provides a standardised approach to assessing cybersecurity risks and developing effective mitigation strategies. Its primary objectives include helping U.K. public sector organisations gain a clear understanding of their cybersecurity posture, identifying and prioritising areas for improvement and evaluating progress over time.

Objective A: Managing security risk

Risk management is an integral part of organisations' defences, and having comprehensive organisational structures, policies and processes is critical to enable public sector organisations to effectively manage and mitigate cybersecurity risks. An effective governance framework helps U.K. public sector organisations identify and protect critical information systems and assets, and also helps organisations maintain the confidentiality, integrity and availability of their data and networks. The implementation of effective risk management requires organisations to have a defined and systematic approach to identifying and assessing security threats, prioritising risks and implementing mitigation measures. The risks organisations face extend beyond traditional boundaries, which now also extend to managing the supply chain, as vulnerabilities in third-party systems can impact the security of an entire organisation. By incorporating robust risk management, asset management, governance and supply chain considerations into their structure, organisations can ensure the protection of their essential functions and minimise the impact of potential security incidents.

Objective B: Protecting against cyberattacks

Defining and communicating clear organisational policies and processes is critical for securing systems and data that support essential functions. These policies and processes should cover key areas such as identity and access controls, data security, system security, resilient networks and systems, and staff awareness and training. By clearly communicating these policies and processes, organisations ensure that all stakeholders understand their role in maintaining the security of the organisation. This includes maintaining proper controls to prevent unauthorised access to systems and data, protecting sensitive information through robust data security measures, implementing system security protocols to safeguard against threats, maintaining the resilience of networks and systems to minimise downtime, and providing staff with the necessary training to identify and respond to potential security incidents. By integrating these measures into their security framework, organisations can effectively secure their systems and data, and protect the confidentiality, integrity and availability of their information.

Objective C: Detecting cybersecurity events

The importance of security monitoring and proactive security event monitoring in organisations cannot be overstated. These capabilities are crucial in ensuring the protection of an organisation's essential functions against evolving and sophisticated cyber threats. Without effective monitoring and event detection systems, organisations risk falling victim to cyberattacks that can lead to loss of sensitive data, disruption of their operations, and harm to their reputation. By having a comprehensive security monitoring program in place, organisations can stay ahead of potential security incidents and detect them quickly. Proactive security event monitoring involves constantly monitoring the environment for signs of unusual activity and taking appropriate measures to prevent or respond to incidents. This proactive approach helps maintain the confidentiality, integrity and availability of essential functions and ensure security defences remain effective.

Objective D: Minimising the impact of security incidents

It is integral for organisations to be able to detect and respond to security incidents while minimising their impact and ensuring critical business processes remain unimpeded. A key component is having a well-defined response and recovery plan and incorporating lessons learned to improve the overall security posture of the organisation. To effectively respond to and recover from a security incident, organisations must ensure they have the required skills and tools to support any incident. As part of their incident response readiness, organisations must take steps to identify, contain and resolve issues, and restore normal operations as quickly as possible. Organisations also need to have working backups of critical systems and data to ensure they can quickly restore normal operations in the event of a cyberattack. Furthermore, it is imperative for organisations to continuously learn from security incidents and incorporate lessons learned into their overall security posture. .

How CrowdStrike Accelerates Alignment with the NCSC CAF

CrowdStrike's suite of services and solutions is expertly designed to help organisations address the NCSC CAF requirements. These offerings assist in the swift and efficient implementation and management of cybersecurity measures that are tailored to the unique requirements of individual organisations.

The following are the key accelerators provided by CrowdStrike, both through product modules (built on the Falcon platform) and through professional services, which help organisations identify risk, improve protection, better detect threats and enhance the resilience of networks and information systems that support essential functions.

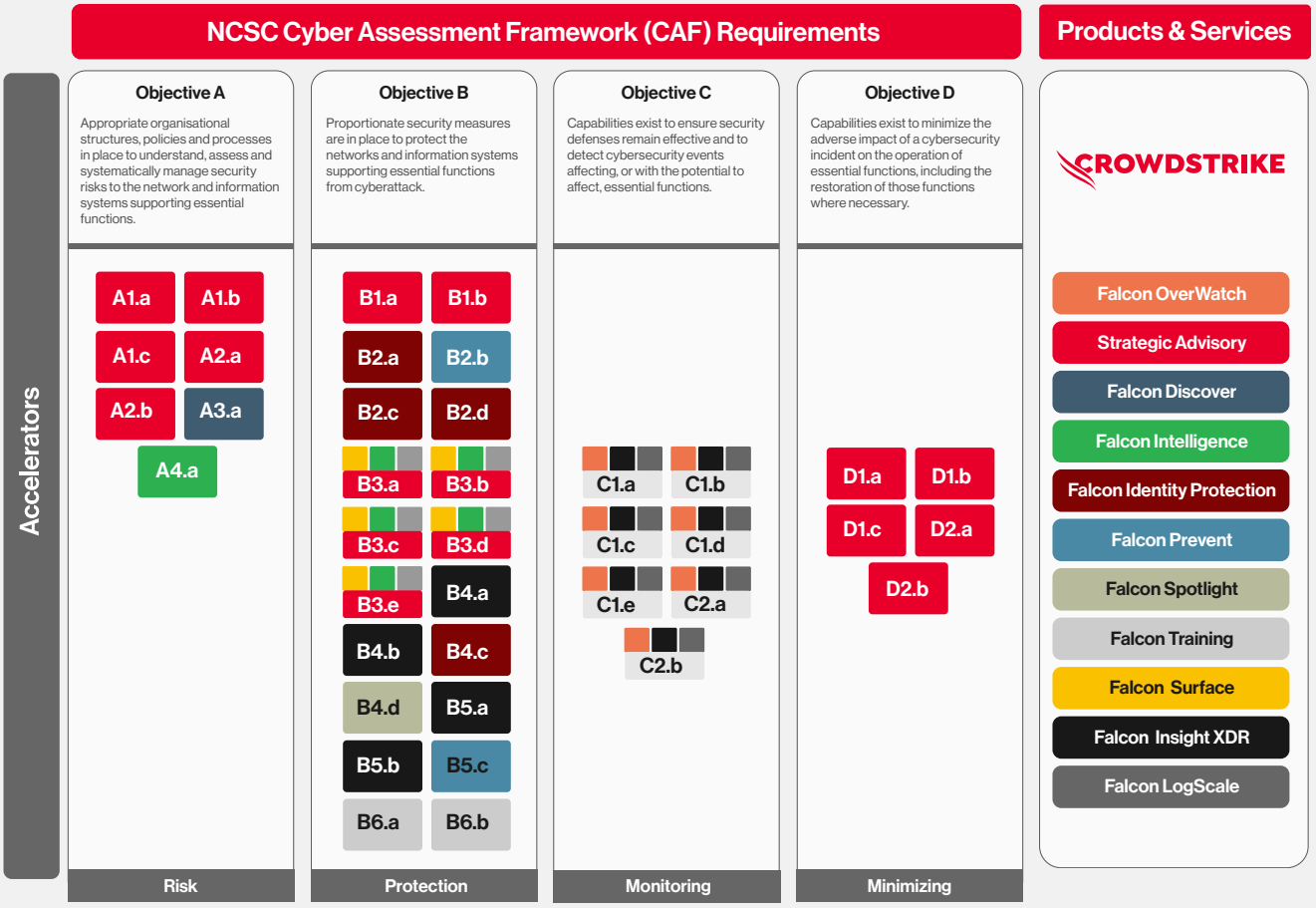

Figure 1: A mapping of CrowdStrike products and services to the NCSC CAF

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective A: Managing Security Risk		
A1: Governance Putting the policies and processes in place to govern the approach to securing network and information systems.	Effective security of network and information systems must be driven by the management team within an organisation and supported by corresponding policies and practices. It is of paramount importance as part of A1 that organisations within the U.K. public sector establish clear governance structures with well-defined lines of responsibility and accountability for ensuring the security of critical systems, networks and data. Establishing a well-defined governance framework empowers organisations to do the following: ▌Effectively define security governance and ensure it is implemented across the organisation. ▌Ensure lines of responsibility and accountability are well defined across the organisation's governance. ▌Ensure flexibility in implementing governance measures appropriate to the organisation's size and complexity.	**CrowdStrike Security Program In-Depth Assessment** helps organisations holistically mature their information security program to a level appropriate for their business risk. The assessment methodology has been developed based upon many years of combined consultant and practitioner experience in conjunction with CrowdStrike's incident response and threat intelligence expertise. **Falcon Intelligence**: CrowdStrike Falcon® Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one.
A2: Risk Management Identify, assess and understand security risks and establish an overall organisational approach to risk management.	The CAF risk management guidance provides organisations with a clear understanding of service dependencies to manage security risks to the network and information systems that support essential functions. This includes identifying physical assets, software, data, essential staff and utilities that are critical to the delivery of essential functions. Implemented effectively, organisations are able to demonstrate the following: ▌A consistent overall organisational approach to risk management. ▌The ability to identify and assess security risks to the network and information systems supporting essential functions. ▌Provide advice and guidance on steps required to appropriately manage the identified security risks. ▌A cohesive and well-informed understanding of the threat landscape. ▌Embed data from various sources (such as the NCSC, sector-specific information exchanges, and government, commercial, and open sources) to gain situational awareness of risks. ▌Engage with wider industry verticals to help with the understanding of threats and vulnerabilities facing their sector. ▌Established a systematic process to manage identified risks effectively. ▌Provide confidence across the organisation that risk mitigations are working effectively.	**CrowdStrike Security Program In-Depth Assessment** helps organisations holistically mature their information security program to a level appropriate for their business risk. The assessment methodology has been developed based upon many years of combined consultant and practitioner experience in conjunction with CrowdStrike's incident response and threat intelligence expertise. **CrowdStrike Technical Risk Assessment** is designed to help organisations gain real-time visibility into who and what is in their network. The CrowdStrike Technical Risk Assessment team leverages the Falcon platform to understand how systems and accounts are being used. This engagement supports Windows Active Directory environments only.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective A: Managing Security Risk		
A3: Asset Management Understanding which systems/ services are required to maintain or support essential functions.	A well-defined asset management solution is of utmost importance for organisations, as it plays a critical role in enabling effective risk management and ensuring the seamless operation of essential functions. By having a clearly defined asset management solution, organisations are equipped to effectively manage risks, comprehend dependencies and safeguard the security and resilience of essential functions. It is crucial to consider all pertinent assets, including those within the operational technology environment, to tailor the approach accordingly and address specific requirements. This tailored approach ensures organisations prioritise safeguarding of critical assets. The guidance emphasises the importance of determining and comprehending all the elements essential for the operation of networks and information systems supporting an organisation's crucial functions. By establishing a clear understanding of service dependencies, organisations can effectively manage security risks and ensure the smooth functioning of their critical operations, which helps them achieve the following: ▌Enhanced risk management processes ▌Improved cyber resilience ▌Streamlined incident response processes ▌Efficient resource allocation ▌Adherence to regulatory compliance	**Falcon Discover**: For IT and security teams that need to identify and track computers and applications on their network, CrowdStrike Falcon® Discover is the CrowdStrike IT hygiene solution. Falcon Discover monitors and inventories systems, application usage and user account usage in real time. **Falcon Forensics**: CrowdStrike Falcon® Forensics is CrowdStrike's powerful triage data collection solution. It allows incident responders to react more quickly to investigations and conduct compromise assessments, threat hunting and monitoring. **Falcon Discover for IoT**: With CrowdStrike Falcon® Discover for IoT, you get in-depth industrial control system (ICS) context, including data such as component type, protocols in your environment, the security zones the assets belong to, IP or MAC addresses within the asset, and what the devices are communicating with. **Falcon Surface:** CrowdStrike® Falcon Surface™ is the industry's most complete adversary-driven external attack surface management (EASM) technology that stops breaches by minimising risk from exposed assets. Falcon Surface pinpoints unknown, exposed internet-facing assets so security teams can secure their ever-evolving digital perimeter.
A4: Supply Chain Understand and manage risks that arise from dependencies on external suppliers.	The CAF guidance highlights the importance of understanding and managing security risks that arise from dependencies on external suppliers in the context of networks and information systems. It is essential for organisations to effectively address supply chain-related security considerations. Some of the key business outcomes of establishing well-documented and understood supply chain policies and procedures include the following: ▌Gaining the ability to understand and manage security risks arising from dependencies on external suppliers. ▌Ensuring accountability for essential functions, even when relying on third-party suppliers. ▌Ensuring contractual agreements with third-party suppliers include provisions for the protection of all critical assets that are managed on behalf of the organisation or are critical for the organisation's essential functions. ▌Providing assurances that data is adequately protected from unauthorised access, modification or deletion that could adversely impact essential functions. ▌Effectively specifying the security properties that are essential for protecting the critical systems, assets or data when procuring products or services from third parties, ▌Having confidence in trustworthy third-party suppliers to manage malicious attempts aimed at subverting the security of products or systems that could impact essential functions.	**CrowdStrike Security Program In-Depth Assessment** helps organisations holistically mature their information security program to a level appropriate for their business risk. The assessment methodology has been developed based upon many years of combined consultant and practitioner experience in conjunction with CrowdStrike's incident response and threat intelligence expertise. **CrowdStrike Technical Risk Assessment** is designed to help organisations gain real-time visibility into who and what is in their network. The CrowdStrike Technical Risk Assessment team leverages the Falcon platform to understand how systems and accounts are being used. This engagement supports Windows Active Directory environments only.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective B: Protecting Against Cyberattacks		
B1: Service Protection Policies and Processes Defining and communicating appropriate organisational policies and processes to secure systems and data.	Comprehensive service protection policies and associated processes are essential for securing network and information systems that support essential functions. A well-defined set of service protection policies and processes is vital for securing all parts of the organisation. By tailoring policies, validating implementation, considering human behaviour, gaining senior management support, providing practical guidance, addressing compliance and adopting a people-focused approach, organisations can enhance security and ensure the following resilience-based outcomes: ▌Having a clear direction for securing systems and data that support essential functions. ▌Crafting policies and processes with the intended target audience in mind for effective communication and understanding of security expectations at different levels within the organisation. ▌Establishing mechanisms to validate the implementation and effectiveness of policies and processes. ▌Understanding data flows for critical services while being able to apply the right level of protection profiles. ▌Adhering to compliance regulations with sector regulations and standards. ▌Allowing for continuous improvement by regularly reviewing and improving security resilience.	**CrowdStrike Security Program In-Depth Assessment** helps organisations holistically mature their information security program to a level appropriate for their business risk. The assessment methodology has been developed based upon many years of combined consultant and practitioner experience in conjunction with CrowdStrike's incident response and threat intelligence expertise.
B2: Identity Access Control Understanding, documenting and controlling access.	The CAF places great emphasis on the concept of verification, which is crucial for maintaining a secure environment for network and information systems. It involves defining authorised interactions and access to sensitive data, mitigating risks, and protecting valuable assets. Key outcomes related to identity-based controls within the CAF include the following: ▌The ability to have a clear understanding and management of identities across the organisation. ▌Assurances that user access rights are granted on principles such as least privilege. ▌Assurances that users, devices and systems are subject to appropriate verification, authentication and authorisation processes before being granted access to data or services. ▌Ability to implement robust identity and access control measures to prevent unauthorised individuals from accessing data or services. ▌In addition to technical security measures, the ability to protect physical access to networks and information systems.	**Falcon Identity Threat Protection**: CrowdStrike Falcon® Identity Threat Protection, a module of the Falcon platform, enables frictionless security with real-time threat prevention and IT policy enforcement using identity, behavioural and risk analytics. **Falcon Elite**: CrowdStrike Falcon® Elite endpoint and identity protection stops breaches by combining next-generation antivirus (NGAV), endpoint detection and response (EDR), real-time identity protection, managed threat hunting, integrated threat intelligence and IT hygiene. **Falcon Prevent**: CrowdStrike Falcon® Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **CrowdStrike Active Directory Security Assessment**: A CrowdStrike Active Directory Security Assessment is a unique offering designed to review your Active Directory configuration and policy settings to reveal security configuration issues that attackers can leverage.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective B: Protecting Against Cyberattacks		
B3: Data Security Protecting stored or electronically transmitted data from actions that may cause an adverse impact.	Data stored or transmitted electronically plays a pivotal role in the operation of essential functions within an organisation. Therefore, it is crucial to ensure that this data is adequately protected from unauthorised access, modification or deletion, as any adverse impact can disrupt the smooth functioning of these critical processes. Data protection extends beyond simply securing its storage or transmission. It also encompasses the means by which authorised users, devices and systems access the critical information necessary for the operation of essential functions. By implementing robust security measures, organisations can safeguard the integrity, confidentiality and availability of their data, mitigating the risk of adverse consequences. Correctly implemented, organisations have the ability to do the following: ▌Implement measures to prevent unauthorised access to sensitive information to ensure the confidentiality of data. ▌Protect data integrity and availability, which is crucial for the operation of essential functions. ▌Ensure adequate security controls are in place for the secure transmission of sensitive data. ▌Validate networks and information systems are designed with data protection in mind. ▌Adequately secure data stored temporarily or permanently from unauthorised access, tampering or deletion. ▌Securely destroy data once it has passed its defined retention prions and is rendered unrecoverable.	**CrowdStrike Security Program In-Depth Assessment** helps organisations holistically mature their information security program to a level appropriate for their business risk. The assessment methodology has been developed based upon many years of combined consultant and practitioner experience in conjunction with CrowdStrike's incident response and threat intelligence expertise. **Falcon Discover**: For IT and security teams that need to identify and track computers and applications on their network, Falcon Discover is the CrowdStrike IT hygiene solution. Falcon Discover monitors and inventories systems, application usage and user account usage in real time. **Falcon Spotlight**: Falcon Spotlight provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritisation for IT analysts. **Falcon Intelligence**: Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Identity Threat Protection**: Falcon Identity Threat Protection, a module of the Falcon platform, enables frictionless security with real-time threat prevention and IT policy enforcement using identity, behavioural and risk analytics. **Falcon FileVantage**: CrowdStrike Falcon® FileVantage, CrowdStrike's file integrity monitoring (FIM) solution, offers central visibility around changes made to critical configuration, system and content files as well as critical folders and registries across your entire organisation.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective B: Protecting Against Cyberattacks		
B4: System Security Protecting networks, systems and technology from cyberattacks.	Protecting critical networks and information systems is paramount. To thwart cyberattacks and preserve system integrity, organisations must grasp the associated risks while ensuring robust security measures are in place to detect and respond to cyberattacks. Security teams should design resilient systems and networks that provide the assurances required when safeguarding vital functions. The use of resilient and layer security architecture design principles helps protect organisations from attack. Adopting a "secure by default" design philosophy is pivotal. It ensures immediate security activation, diminishing vulnerabilities and deterring attacks. Imposing stringent access controls and disabling unnecessary services amplifies security and allows organisations to do the following: ▌Provide enhanced protection controls for critical networks and information systems to defend against cyberattacks. ▌Increase cyber resilience and continuity of critical data, assets, systems and networks. ▌Gain a greater understanding of cyber risks and vulnerabilities within the organisation. ▌Enforce principles of least privilege and identity isolation. ▌Provide the ability to effectively detect unauthorised attempts to circumvent security measures. ▌Implement a robust patch management process across the organisation. ▌Apply segmentation controls across the organisation to ensure assets requiring higher levels of segmentation are protected from those requiring a lesser set of security controls.	**Falcon OverWatch**: Falcon OverWatch is CrowdStrike's managed threat hunting service built on the CrowdStrike Falcon platform. Falcon OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies. **Falcon Intelligence**: CrowdStrike Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Insight XDR**: CrowdStrike Falcon® Insight XDR extends CrowdStrike's industry-leading EDR capabilities and delivers real-time, multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. **Falcon Prevent**: Falcon Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **Falcon Discover**: For IT and security teams that need to identify and track computers and applications on their network, Falcon Discover is the CrowdStrike IT hygiene solution. Falcon Discover monitors and inventories systems, application usage and user account usage in real time. **Falcon Surface**: CrowdStrike Falcon Surface is the industry's most complete adversary-driven EASM technology that stops breaches by minimising risk from exposed assets. Falcon Surface pinpoints unknown, exposed internet-facing assets so security teams can secure their ever-evolving digital perimeter.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective B: Protecting Against Cyberattacks		
B5: Resilient Networks and Systems Building resilience against cyberattacks.	Organisations must prioritise the resilience of their core functions against cyberattacks. While technical protection is crucial (as highlighted in B4), it is equally important to consider how operations can continue in the event of technology failure or compromise. This encompasses not only the robustness of the technology itself but also the implementation of contingency measures — such as manual processes — to ensure uninterrupted function. To be well prepared for significant disruptions, organisations should have robust business continuity and disaster recovery plans in place to enable them to do the following: ▌Ensure resilience is built into aspects of essential functions against cyberattacks. ▌Minimise the impact and disruption caused by technology failures or compromise. ▌Apply the right level of protection for devices and interfaces used for administration against targeted attacks. ▌Be prepared to respond to significant disruptions through business continuity, disaster recovery planning and incident response plans. ▌Leverage a diverse set of technologies and geographic locations for resilience. ▌Ensure that working backups for hardware and data can be established in the event of an outage. ▌Enforce physical security controls across their physical estate.	**Falcon OverWatch**: Falcon OverWatch is CrowdStrike's managed threat hunting service built on the CrowdStrike Falcon platform. Falcon OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies. **Falcon Intelligence**: CrowdStrike Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Insight XDR**: CrowdStrike Falcon Insight XDR extends CrowdStrike's industry-leading EDR capabilities and delivers real-time, multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. **Falcon Prevent**: Falcon Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **Falcon Discover**: For IT and security teams that need to identify and track computers and applications on their network, Falcon Discover is the CrowdStrike IT hygiene solution. Falcon Discover monitors and inventories systems, application usage and user account usage in real time. **Falcon Surface**: CrowdStrike Falcon Surface is the industry's most complete adversary-driven EASM technology that stops breaches by minimising risk from exposed assets. Falcon Surface pinpoints unknown, exposed internet-facing assets so security teams can secure their ever-evolving digital perimeter.
B6: Staff Awareness and Training Supporting staff to ensure they make a positive contribution toward cybersecurity.	To effectively protect their networks and information systems, it is crucial for these organisations to prioritise staff awareness and training. Staff members play a pivotal role in maintaining the security of essential functions, and ensuring they have the necessary awareness, knowledge and skills is paramount. Effective security awareness enables organisations to do the following: ▌Enhance staff awareness, knowledge and skills when responding to a security incident. ▌Integrate a security culture throughout the organisation. ▌Offer tailored security awareness and training programs that align with responding to potential security issues. ▌Conduct continuous security awareness initiatives to maintain and reinforce cybersecurity requirements. ▌Accommodate different learning preferences and delivery methods to maximise training uptake. ▌Instill a positive security culture where staff are aware of their role in maintaining security and actively contribute to improving it.	**CrowdStrike University**: CrowdStrike University offers a Customer Access Pass program to eligible customers to ensure that users of the CrowdStrike Falcon platform can take full advantage of CrowdStrike's ability to stop breaches. The Customer Access Pass provides access to the CrowdStrike University online learning portal, where organisations can benefit from a large library of CrowdStrike eLearning courses and product update videos at no charge.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective C: Detecting Cybersecurity Events		
C1: Security Monitoring Monitoring to detect potential security problems and track the effectiveness of existing security measures.	Maintaining a secure environment for critical operations necessitates ongoing monitoring of network and system security. This enables the timely detection of potential security issues and ensures the effectiveness of protective measures. Comprehensive security monitoring enables organisations to have safeguarding controls in place against known and unknown threats. By collecting and aggregating logs, organisations gain situational awareness, allowing them to identify anomalies and suspicious activities. Monitoring and analysis tools, along with **indicators of attack (IOAs)**, aid in the detection of — and response to — security incidents. Correctly implemented, organisations can do the following: ▌Implement an effective monitoring strategy. ▌Undertake timely identification of security breaches through skilled analysis. ▌Continuously review and maintain security measures to ensure their ongoing effectiveness. ▌Prioritise monitoring efforts for assets and systems supporting essential functions to mitigate potential adverse impacts. ▌Ingest data from multiple data sets into a single platform. ▌Comply with legal data protection laws when collecting and storing log information. ▌Utilise monitoring and analysis tools to effectively correlate and investigate security events. ▌Validate and update monitoring strategies and capabilities to align with evolving business requirements.	**Falcon OverWatch**: Falcon OverWatch is CrowdStrike's managed threat hunting service built on the CrowdStrike Falcon platform. Falcon OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies. **Falcon Insight XDR**: CrowdStrike Falcon Insight XDR extends CrowdStrike's industry-leading EDR capabilities and delivers real-time, multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. **Falcon Intelligence**: CrowdStrike Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Prevent**: Falcon Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **Falcon LogScale**: CrowdStrike Falcon® LogScale gives IT teams a single platform that can store, analyse and retain all log and event data at petabyte scale. Falcon LogScale minimises the computing and storage resources required to ingest, search, transform and retain log data.
C2: Proactive Security Event Discovery Detecting anomalous events in relevant network and information systems.	The ability to detect malicious activity within networks and information systems is crucial for safeguarding the operation of critical functions of an organisation. An essential aspect of C2 is the detection and analysis of unusual anomalous data streams. By scrutinising network patterns and identifying abnormal communication flows, organisations can uncover potential indicators of compromise and take appropriate action. Correctly implemented, organisations are able to do the following: ▌Detect malicious activity and anomalous events. ▌Identify deviations from normal system interactions. ▌Design network and information systems with proactive security event discovery in mind. ▌Adopt proactive monitoring approaches based on heuristic analysis, leveraging knowledge of past attacks, system behaviour and comprehensive understanding of threat intelligence.	**Falcon OverWatch**: Falcon OverWatch is CrowdStrike's managed threat hunting service built on the CrowdStrike Falcon platform. Falcon OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies. **Falcon Insight XDR**: CrowdStrike Falcon Insight XDR extends CrowdStrike's industry-leading EDR capabilities and delivers real-time, multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. **Falcon Intelligence**: CrowdStrike Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response, and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Prevent**: Falcon Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **Falcon LogScale**: Falcon LogScale gives IT teams a single platform that can store, analyse and retain all log and event data at petabyte scale. Falcon LogScale minimises the computing and storage resources required to ingest, search, transform and retain log data.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective D: Minimising the Impact of Security Incidents		
D1: Response and Recovery Planning Putting suitable incident management and mitigation processes in place.	The establishment of well-defined and tested incident management processes is of utmost importance, as it serves the vital purpose of ensuring the continuity of essential functions when confronted with system or service failure. It is imperative to ground your organisation's incident response plans in thorough and comprehensive risk assessments that have been documented as part of your organisation's risk assessment process (A2). Correctly implemented, organisations can do the following: ▌Implement well-defined and tested incident management processes to ensure continuity of essential functions during system or service failures. ▌Adopt mitigation activities to contain or limit the impact of compromise on essential functions. ▌Understand and comply with mandatory incident reporting requirements. ▌Validate that the incident response plan is grounded in thorough risk assessment findings, is integrated into all business functions, ensures interoperation between the incident response and security monitoring functions, and considers incidents involving suppliers and the wider supply chain. ▌Develop clear governance frameworks, roles and procedures for reporting incidents to internal and external stakeholders, such as regulators and competent authorities. ▌Validate incident response capabilities through exercises that reflect past experiences, red teaming, scenario planning and risk assessments. ▌Document lessons learned from exercises and ensure all uplifting initiatives are implemented accordingly.	**Falcon OverWatch**: Falcon OverWatch is CrowdStrike's managed threat hunting service built on the CrowdStrike Falcon platform. Falcon OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies. **Falcon Insight XDR**: CrowdStrike Falcon Insight XDR extends CrowdStrike's industry-leading EDR capabilities and delivers real-time, multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. **Falcon Intelligence**: CrowdStrike Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Prevent**: Falcon Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **Falcon LogScale**: Falcon LogScale gives IT teams a single platform that can store, analyse and retain all log and event data at petabyte scale. Falcon LogScale minimises the computing and storage resources required to ingest, search, transform and retain log data. **CrowdStrike Incident Response**: The CrowdStrike Incident Response team works collaboratively with organisations to handle critical security incidents, resolve immediate issues and implement a long-term solution to stop recurrences. The Incident Response team takes an intelligence-led, teamwork-driven approach to investigations, blending real-world incident response and remediation experience with cutting-edge technology via the unique, cloud-based Falcon platform.

CAF Principle	Interpretation of the CAF requirements and identification of potential business outcomes	How to demonstrate meeting these outcomes through CrowdStrike products and services
Objective D: Minimising the Impact of Security Incidents		
D2: Lessons Learnt Learning from incidents and implementing these lessons to improve resilience.	When an incident occurs, it is crucial for an organisation to extract valuable lessons from it and take necessary measures to prevent its recurrence. Organisations should focus on addressing the root cause. This approach allows them to improve overall resilience while ensuring the following: ▌The ability to conduct root cause analysis of the incident. ▌Implement measures to prevent similar incidents from occurring in the future. ▌Retain sufficiently detailed records to identify the root causes of incidents. ▌Incorporate adequate documentation of lessons learned into comprehensive response plans. ▌Share lessons learned during a security incident with relevant internal and external stakeholders.	**Falcon OverWatch**: Falcon OverWatch is CrowdStrike's managed threat hunting service built on the Falcon platform. Falcon OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies. **Falcon Insight XDR**: CrowdStrike Falcon Insight XDR extends CrowdStrike's industry-leading EDR capabilities and delivers real-time, multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. **Falcon Intelligence**: CrowdStrike Falcon Intelligence is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response and enabling security teams to move from a reactive state to a predictive, proactive one. **Falcon Prevent**: Falcon Prevent endpoint protection delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. **Falcon LogScale**: Falcon LogScale gives IT teams a single platform that can store, analyse and retain all log and event data at petabyte scale. Falcon LogScale minimises the computing and storage resources required to ingest, search, transform and retain log data. **CrowdStrike Incident Response**: The CrowdStrike Incident Response team works collaboratively with organisations to handle critical security incidents, resolve immediate issues and implement a long-term solution to stop recurrences. The Incident Response team takes an intelligence-led, teamwork-driven approach to investigations, blending real-world incident response and remediation experience with cutting-edge technology via the unique, cloud-based Falcon platform.

Conclusion

The U.K. public sector has grown increasingly reliant on digital technologies, yet these organisations face a mounting number of sophisticated and persistent cyber threats. Therefore, it is crucial for these organisations to put appropriate security measures in place to safeguard against these risks. CrowdStrike's advanced technology and human expertise offer U.K. organisations the necessary tools to mitigate security risks and protect against cyber threats.

By leveraging CrowdStrike's comprehensive suite of security and advisory solutions, U.K. organisations can gain a deeper understanding of their risk appetite, safeguard themselves against cyberattacks, detect security incidents and minimise the impact of security threats. One-time compliance exercises fall short, whereas CrowdStrike solutions provide continuous situational awareness of the threats clients face. CrowdStrike stands out as an exemplary partner that many U.K. business sectors trust to help their organisation align with the NCSC CAF and enhance compliance with regulations such as the NIS Directive and GovAssure.

CrowdStrike's portfolio of products and services align seamlessly with the NIS/CAF objectives and principles. CrowdStrike solutions are designed for speed, simplicity and scale, ensuring seamless detection and response capabilities to effectively tackle the constantly evolving threat landscape — all while providing customers with the following:

- Strategic, tactical and operational intelligence to enable the right risk-based decisions
- Protection across a dispersed attack surface, including endpoint, cloud, network, identity and data domains
- Detection of risks and security incidents in real time
- Support for incident response, remediation and recovery of critical business functions after an incident

With the use of products such as CrowdStrike Falcon Insight XDR, U.K. organisations can transcend traditional detection and response methods and harness the full capabilities of the next-generation, extended detection Falcon platform, which is powered by a single lightweight agent through a centralised console. CrowdStrike's advanced suite of products and services enables organisations to meet and mitigate the threat[1], gain enhanced visibility across the enterprise, and more simply manage their security posture from a single-pane interface.

Achieving strong cybersecurity practices and maturity requires an integrated approach, where principles complement each other and solutions can fulfil multiple requirements simultaneously. CrowdStrike, a trusted partner of many public sector organisations, is dedicated to supporting the U.K. public sector, CNI and associated organisations in safeguarding against the constantly evolving threat landscape posed by highly sophisticated threat actors. By providing comprehensive endpoint protection with real-time threat detection and response capabilities, CrowdStrike's cloud-based Falcon platform has made it easier for organisations to do the following:

- Manage cyber risk
- Protect against cyberattacks
- Detect cybersecurity incidents
- Minimise the impact of cyber incidents

[1] CrowdStrike 2023 Global Threat Report

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**