The Cyber Assessment Framework

Examining the role of the Cyber Assessment Framework from the perspective of Identity Security.

DAVID TYRRELL
PRINCIPAL SOLUTIONS CONSULTANT

The Cyber Assessment Framework

The National Cyber Security Centre produced the Cyber Assessment Framework (CAF) for the use of organisations that play a vital role in the day-to-day life of the UK.

The CAF collection is aimed at helping an organisation achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified essential functions performed by that organisation.

The CAF collection is written primarily in terms of outcomes to be achieved rather than a compliance checklist. There will often be different ways of achieving the specified CAF outcomes, which could give rise to uncertainty about the extent to which an organisation has successfully put in place an appropriate level of cyber resilience. However, the inclusion of Indicators of Good Practice (IGPs) in the CAF provides a guide to the type of measures that would normally be present in an organisation that was achieving CAF outcomes, allowing that organisation to demonstrate the appropriate level of cyber resilience.

The purpose of this document is to summarise where SailPoint, the leader in Identity Security, can assist organisations achieve their goals towards demonstrating cyber resilience within the context of the CAF.

Why is Identity Security critical to cyber resilience?

The Government's "Cyber security breaches survey 2024" states that 74% of large UK businesses report having experienced some form of cyber security breach or attack in the last 12 months, and the most common type of breach or attack by far is phishing, with 84% of businesses experiencing an attack.

These identity-based attacks are easy to launch and can be perpetrated by lone scammers, sophisticated criminal gangs or even nation states. The goals are to steal credentials, data, or to place malware on devices. Making breaches even harder to avoid, AI is transforming phishing techniques, with skilled and unskilled actors using generative AI to improve and amplify their attacks. Deepfake videos and audio generated by AI are becoming increasingly difficult to discern.

Let's examine some of the CAF Objectives, and the key principles related to identity security. At the time of writing, the CAF was at Version 3.2.

CAF Objective A – Managing Security Risk

Principle A4 Supply Chain

The risk of supply chain compromise continues to loom large, and a chain is only as strong as its weakest link. It is essential that suppliers, contractors and other third parties have timely access to the systems and data they need. It is also critical that this access is restricted, monitored and subject to the same security controls as regular employees. But many organisations lack the necessary processes or technology to achieve this.

CAF "Not Achieved" statements include:

- "*You do not know what data belonging to you is held by suppliers, or how it is managed.*"
- "*Suppliers have access to systems that provide your essential function(s) that is unrestricted, not monitored or bypasses your own security controls.*"

At the heart of this problem, it is quite common that contractors fall outside of normal HR processes, and the access of suppliers and other third parties may be managed with spreadsheets or helpdesk tickets.

This results in common access governance challenges:

- **Audit difficulties** – unable to show what contractors had access to, or why
- **Inefficient processes** – takes too long to onboard external people
- **High risk** – third parties leave but access is not removed

SailPoint extend advanced identity security controls, so you have the same visibility with non-employees as you do with your employees.

SailPoint Non-Employee Risk Management provides operational efficiency and minimises risk by dynamically informing you exactly which non-employees need access, why they require it, and when it's appropriate.

Identity repository	Centralised and scalable repository for all nonemployees
Non-employee record	Reliable identity data to meet your IAM strategy
Strengthens security	Full visibility into your non-employees and their access
Process orchestration	Flexible workflows for onboarding, offboarding, and daily lifecycle management
Enables collaboration	Both internal and external users can collect non-employee data
Simplifies audits	Captures essential identity data and documents the entire non-employee lifecycle

With SailPoint Non-Employee Risk Management and SailPoint Identity Security Cloud, you can manage the simplest to the most complex scenarios when it comes to non-employee identities the same way you manage employee identities.

CAF Objective B – Protecting against cyber attacks

Principle B2 Identity and Access control

The CAF principle states that *"It is important that the organisation is clear about who (or what in the case of automated functions) has authorisation to interact with the network and information systems supporting an essential function in any way or access associated sensitive data. Access rights granted should be carefully controlled, especially where those rights provide an ability to materially affect the operation of the essential function. Access rights granted should be periodically reviewed and technically removed when no longer required such as when an individual changes role or leaves the organisation."*

CAF is talking here about the fundamentals of identity security. It is vital that users have the least amount of privilege necessary to perform their duties. In the event of a breach, we want the blast radius to be as small as possible. Intruders will attempt to access all the data they can, and if possible, move laterally within the network. By ensuring users do not have excessive levels of access, this is much harder to do.

However, keeping track of who has access to what, ensuring movers do not accumulate access as they change role, and removing access immediately when necessary is not easy in today's complex IT landscapes, and has arguably moved beyond human ability.

CAF indicators of good practice (IGPs) include:

- *Not achieved: The number of authorised users and systems that have access to your network and information systems are not limited to the minimum necessary.*
- *Achieved: The list of users and systems with access to network and information systems supporting and delivering the essential function(s) is reviewed on a regular basis, at least every six months.*

SailPoint provides a 360° view of who (or what) has access to what, across all applications and data, for all employees and non-employees. From this vantage point, it's easier to track movers and leavers, and to perform reviews of essential functions on a periodic basis. To make this feasible, AI is used to make recommendations, focusing your limited time available on high-value decisions.

SailPoint Identity Security Cloud revolutionises identity security for organisations by:

Empowering precision access:

- Grant every identity precise and timely access through a Least Privilege Access (LPA) model.
- Elevate productivity by ensuring that everyone has the appropriate level of access without compromising security.

Identity Risk Management:

- Equip security professionals with tools to identify and manage potential identity & access risks.
- Enhance your security posture by staying ahead of threats and vulnerabilities, minimising the impact of potential breaches.

Accelerating Access Decision-Making:

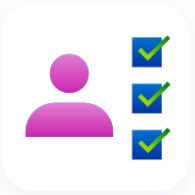
- Enable business managers and application owners to swiftly make informed access decisions.
- Facilitate faster and more effective collaboration across departments with personalised insights and automated workflows.

Simplified Compliance:

- Provide internal auditors with user-friendly tools for easy compliance demonstration.
- Streamline the compliance process, ensuring that audits are seamless, accurate, and demonstrate adherence to regulatory requirements.

Lifecycle Management

Automate and manage joiners, movers, leavers, and access requests



Compliance Management

Streamline access reviews and policy enforcement including SOD

Access Modeling

Create and implement access roles that fit your organization's needs

Analytics

Make better access decisions with actionable insights into identity data

Our experience working with major UK public sector organisations has provided insight into exactly what is needed to ensure users have only the minimum levels of

access needed to perform their jobs: targeted, organised, SaaS-based products that work together as a single, unified solution.

Principle B3 Data Security

Employees are creating, downloading, extracting, copying, and sharing data across an ever-growing digital ecosystem. As a result, the potential attack surface has expanded.

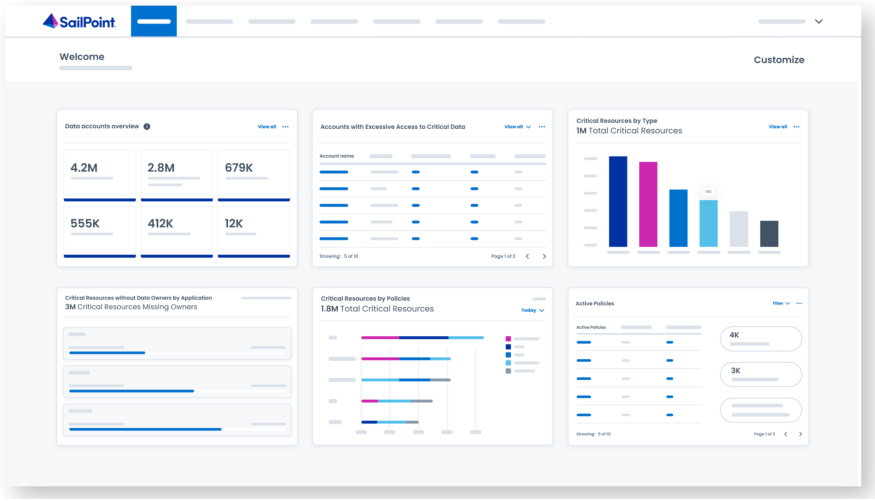
The CAF states that "*As a minimum, unauthorised access to important and critical data should be prevented*".

"Not achieved" IGPs include:

- *You have incomplete knowledge of what data is used by and produced in the operation of the essential function(s).*
- *You have not identified the important data on which your essential function(s) relies.*
- *You have not identified who has access to data important to the operation of the essential function(s).*

SailPoint Data Access Security extends your identity security program by discovering and classifying your sensitive, regulated, and critical data assets within your environment. Data Access Security provides key features to help deliver CAF outcomes:

Data discovery	Discover critical data and sensitive information that is shared or stored across the enterprise
Data classification	Identify and catalogue unstructured data by content analysis, rules, dictionaries, patterns, and custom policies
Permission analysis	See who has access to critical data, how access is granted and shared, and remediate access
Forensic analysis	Capture and export fine-grained details on data access for investigators
Reporting	Track and share detailed reporting for identity hygiene, access risk, and critical data analysis and regulatory compliance
Governance dashboard	Get a centralised view of identity and data security posture and compliance readiness



Data Access Security is integrated into SailPoint's Identity Security Cloud platform, meaning a single solution for governing access to applications and unstructured data.

CAF Objective C – Detecting cyber security events

Principle C2 Proactive security event discovery

"The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/detect solutions."

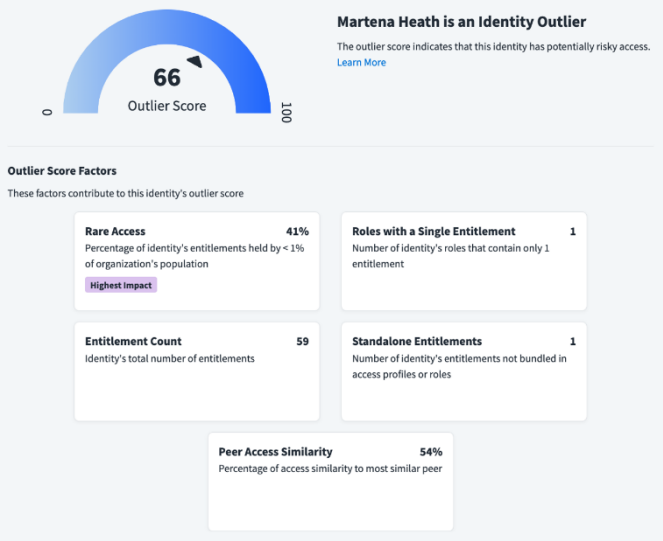
From an identity management perspective, it can be very difficult to look for abnormalities in identity data. When considering the number of applications in use, the number of permissions and entitlements held in those applications, the amount of data held in the organisation, and the number of users accessing it all, the total volume of access intelligence is huge. To make it even harder to analyse, the landscape is dynamic.

As a result, the “Not achieved” IGPs are well known:

- *Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.*
- *You have no established understanding of what abnormalities to look for that might signify malicious activities.*
- *You do not routinely search for system abnormalities indicative of malicious activity.*

SailPoint has built a method for detecting abnormal access using AI and ML.

SailPoint analyses all the access across all users and identifies peer-group patterns. The AI detects identities where their access privilege is not like other identities within their peer-group. The AI tells you who your riskiest users are and initiates risk remediation actions automatically. You may want to notify a security team to investigate or ask their manager to review their access.



This analysis is constantly redone as access changes, people change roles or projects, identifying new abnormalities as they arise, and giving the organisation flexibility in how to respond.

CAF Objective D – Minimising the impact of cyber security incidents

Incidents will invariably happen. When they do organisations should be prepared to deal with them, and as far as possible, have mechanisms in place that minimise the impact on the essential function.

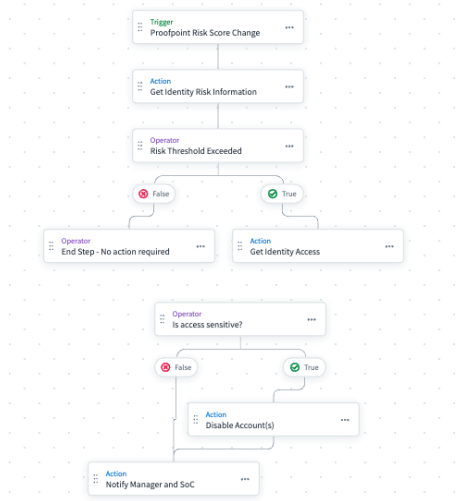
If you want to respond effectively to cybersecurity identity attacks then it’s imperative that you have visibility of who has access to what systems and data,

because in the event of a breach you need to know if a user has access to sensitive or critical data and systems.

SailPoint Risk Connectors makes it easier for organisations to make informed access decisions based on an identity's third-party risk scores. Speed is essential to risk mitigation, especially in the context of delivering secure access to critical data and applications, and SailPoint Risk Connectors is designed to help organisations act quickly if an identity's risk level changes.

SailPoint Risk Connectors consumes third-party risk information from leading vendors like CrowdStrike, Proofpoint, and Elevate Security. With the third-party risk score assigned to identities, organisations can use automation to adapt access according to risk, ensure least-privilege access, and enhance their overall security posture.

SailPoint not only allows the consumption of risk data from other systems, but it enables organisations to visualise the information in the context of identities and their access to execute more informed access decisions quickly. For example, SailPoint's connectivity framework could respond to a risky user by launching a workflow to disable or suspend access or force an access re-certification.



Customers can also view identity risk scores in the SailPoint Access Intelligence Centre to better understand trends or focus on risky user populations. SailPoint is designed to provide the foundation that brings together a holistic view of every enterprise identity, enriching SailPoint's data model with the real-time risk data that customers need to secure their organisation and its data.

Summary

SailPoint's AI-driven security platform provides the autonomous governance that helps solves the needs for organisations seeking to deliver CAF outcomes related to identity security.

CAF Objective	Benefits
Managing Security Risk	• Manage supply chain access to ensure non-employees have the right access to essential functions and data, at the right time
Protecting against cyber attacks	• Ensure all users (and machine identities) have the least privilege necessary to perform their duties. • Periodic access review of essential functions with AI recommendations. • Discover, catalogue and govern sensitive data.
Detecting cyber security events	• Automatically discover abnormal access rights and take appropriate action to review.
Minimising the impact of cyber security incidents	• Take automatic action to reduce the blast radius when risk signals are detected

The SailPoint difference:

- ✓ World-class research and development, analytics, and automation accelerate security and business results
- ✓ Solution flexibility gives you the scalability to tailor identity security to your needs and goals
- ✓ A solution trusted by the world's largest organisations builds confidence and trust
- ✓ Ability to maximise productivity while minimising access privileges optimises impact
- ✓ State-of-the art technologies improve user experience and reduce overall total cost of ownership
- ✓ Outstanding technical training improves implementation and operational success