

**Glasgow Kelvin College**

**Board of Management Meeting of 10 June 2026**

**Cyber Assessment Framework (CAF) Progress Report**

**Report By Assistant Principal of Digital and Information Services**

**1. Introduction**

The purpose of this paper is to provide the Board with an update on the College's progress towards alignment with the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF). This report provides assurance that a structured and evidence-based programme is underway to assess the College's cyber resilience against recognised national standards. A detailed progress report is included at Appendix 1.

**2. Progress Summary**

The College is at an early but well-developed stage in formal CAF alignment. A comprehensive baseline assessment has been completed using a detailed CAF framework, supported by HEFESTIS, and this has identified both areas of strength and targeted areas for further development.

The assessment indicates that:

- Governance, risk management structures and the majority of technical controls are already in place and operating effectively
- The College is broadly aligned with many CAF outcomes, particularly in relation to protection and resilience
- Areas for further development are focused on advancing capability, particularly in relation to:
  - Understanding cyber threats
  - Supply chain assurance
  - Proactive detection and threat hunting

These findings position the College as having a sound cyber security posture, with a clear programme in place to strengthen alignment over the next 12 months.

### **3. Resource Implications**

There are no immediate additional resource requirements arising from this report. However, as the College's alignment with the Cyber Assessment Framework develops, further targeted investment may be required over the medium to longer term to enhance capability in specific areas, particularly in relation to threat intelligence, detection and monitoring, and ongoing cyber resilience.

### **4. Impact on Students**

There are no direct impacts on students arising from this report. However, strengthening cyber resilience supports the continuity and security of learning, teaching and student services.

### **5. Risk and Assurance**

The report provides assurance that cyber risks are being actively identified and managed through a structured framework aligned to national best practice. While the CAF assessment has identified areas for further development, these are targeted and relate primarily to advancing maturity rather than addressing fundamental weaknesses.

### **6. Equality**

No adverse impacts on individuals with protected characteristics have been identified.

### **7. Data Protection**

The work supports the College's data protection framework by strengthening controls, governance and oversight of cyber security risks, ensuring continued compliance with statutory obligations.

### **8. Environmental and Sustainability**

There are no environmental or sustainability implications arising from this report.

### **9. Recommendations**

It is recommended that members:

- i) note the content of this report and the progress outlined in **Appendix 1**.

### **10. Further Information**

Further information can be obtained from Jason Quinn, Assistant Principal, Digital and Information Services. at [jquinn@glasgowkelvin.ac.uk](mailto:jquinn@glasgowkelvin.ac.uk)

**Progress Towards the NCSC Cyber Assessment Framework (CAF)**

Overall, the College is at an early but strong stage in formal CAF alignment, with a structured improvement programme underway and existing assurance indicating a sound cyber security posture.

**1. Purpose**

This paper provides an update on Glasgow Kelvin College's progress towards alignment with the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF). It outlines the College's current level of maturity, the evidence underpinning that position, and the activity undertaken over the past year to strengthen cyber resilience. It also explains the approach currently being taken to assess alignment with CAF in a structured and evidence-based way and how this work aligns with the Scottish Government Cyber Resilience Framework (CRF).

**2. Strategic Context**

The College has taken a deliberate strategic decision to align its cyber security arrangements with the NCSC Cyber Assessment Framework. Although this is not a mandatory requirement, CAF is recognised as the leading UK model for assessing organisational cyber resilience across governance, protection, detection and response. Its adoption reflects a commitment to good governance, proactive risk management and continuous improvement.

CAF is outcome-based, focusing on whether organisations are effectively managing cyber risk in practice, rather than simply implementing controls. The Scottish Government Cyber Resilience Framework is closely aligned to CAF, meaning that progress against CAF directly supports compliance with national public sector expectations and reporting requirements.

**3. Approach to Assessing CAF Alignment**

The College has recently begun a structured programme of work to assess its alignment with CAF in more detail. This work has been undertaken in partnership with HEFESTIS, who provide specialist cyber security expertise to the sector.

The starting point for this work has been a detailed internal assessment using CAF questionnaire. This includes over 560 individual assessment questions aligned to the full CAF framework, covering objectives, principles and contributing outcomes.

As a first pass, the College has worked through the full set of assessment questions to establish a baseline position. This has produced three key outputs:

- A summary assessment of CAF alignment
- A maturity posture view across the CAF objectives and categories
- A CAF-aligned risk register identifying areas requiring improvement

This initial assessment indicates that many CAF outcomes are already either achieved or partially achieved. For example, governance structures, policy frameworks, and many technical controls are assessed as being in place and operating effectively. However, it also highlights areas where improvement is required, including aspects of understanding threats, supply chain assurance, identity and access management, and consistency of control implementation across the organisation.

This work is now being progressed in more depth, again in collaboration with HEFESTIS, who are supporting the College with:

- Validation of the initial assessment
- Provision of sector-aligned templates and guidance
- Development of improvement plans aligned to CAF outcomes

This programme of work is expected to continue over the next 12 months, with a more refined and evidence-based position emerging as the assessment is validated and strengthened.

#### **4. Current Level of Alignment with CAF**

At this stage, it is important to note that the College's position should be understood as developing rather than final. The initial CAF assessment provides a baseline, but further validation work is ongoing.

The early indication from this assessment is that the College is broadly aligned with many of the core CAF outcomes, particularly in the areas of governance, protective controls and resilience. A number of outcomes have initially been assessed as fully achieved, including those relating to senior-level oversight, clearly defined security responsibilities, and the presence of key technical controls.

Some areas are assessed as partially achieved. In particular, the assessment indicates that risk management processes are generally well established and operating effectively. However, there are specific areas where further maturity is required, particularly in relation to:

- Understanding and modelling of relevant cyber threats (CAF A2.b)
- Assurance over supply chain and third-party risks (CAF A4.a)

These findings reflect the need to move beyond established governance processes towards more advanced and intelligence-led risk management.

The current position can therefore be summarised as follows:

| CAF Objective                      | Headline Position            | Commentary                                                                                                                                 |
|------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| A: Managing Risk                   | Largely aligned              | Strong governance and risk structures in place; further maturity required in threat understanding (A2.b) and supply chain assurance (A4.a) |
| B: Protecting Against Cyber Attack | Largely aligned              | Strong technical control environment and policy framework                                                                                  |
| C: Detecting Cyber Security Events | Partially to largely aligned | Monitoring capability established; further development required in proactive threat hunting and analysis                                   |
| D: Minimising Impact of Incidents  | Largely aligned              | Established incident response and recovery arrangements, tested and internally coordinated                                                 |

This table reflects the current high-level view and will be refined as the detailed CAF assessment progresses.

## 5. Supporting Evidence and Assurance

While the detailed CAF assessment is ongoing, the College can draw on a range of existing evidence and external assurance which corroborate the initial findings and indicate a reasonably strong cyber security posture.

The College has well-established governance arrangements, supported by a comprehensive policy framework, including the ICT Security Policy and ICT Acceptable Use Policy. These define expectations for secure system design, user behaviour and access control, and align with recognised good practice.

Operationally, the College maintains a mature technical control environment. This includes endpoint protection, vulnerability management, patching processes and identity and access controls. These are supported by regular scanning, testing and monitoring activities.

Detection capabilities are enhanced through the use of Jisc's Cyber Security Threat Monitoring service, which provides continuous monitoring and external specialist support. This ensures that potential threats can be identified and escalated in a timely manner.

The College also maintains formal incident response and disaster recovery arrangements. These are documented, tested and aligned to recognised frameworks, providing assurance that the College can respond effectively to cyber incidents.

In addition to internal controls, the College benefits from external validation through:

- Internal audit, which has provided a strong level of assurance over cyber security arrangements
- Cyber Essentials certification, confirming the presence of baseline technical controls
- Sector benchmarking through Jisc, providing comparative insight into cyber maturity
- Cyber insurance, providing access to specialist support in the event of a major incident

Taken together, these sources provide confidence that, despite the ongoing CAF assessment, the College already operates from a position of relative strength.

## **6. Activity Undertaken to Strengthen CAF Alignment**

Over the past year, the College has undertaken a range of activity that aligns with CAF principles and supports improved cyber resilience.

Cyber security has been embedded within the Digital Enabler Framework as a core organisational capability. This ensures that cyber resilience is considered as part of wider digital transformation and infrastructure planning.

Governance has been strengthened through continued partnership with HEFESTIS, providing access to specialist expertise and strategic advice through a shared Chief Information Security Officer (CISO) model.

Monitoring and detection capabilities have been enhanced through continued use of Jisc's CSTM service, providing 24/7 operational monitoring and access to sector-wide intelligence.

Incident response arrangements have been updated and continue to be tested through planned exercises. These are supported by formal collaboration with regional college partners, enabling coordinated responses and shared learning across the Glasgow region.

The College has also continued to invest in staff awareness and behavioural controls, including cyber security training and phishing simulation exercises, which support CAF expectations in relation to organisational culture and user behaviour.

## **7. Areas for Further Development**

The initial CAF assessment has identified a number of areas where further work is required. These are not unexpected at this stage and reflect the depth and breadth of CAF as a framework.

Areas for enhancement and further development include:

- Enhancing the College's understanding of cyber threats, including the development of more formal threat intelligence capability
- Strengthening supply chain assurance processes to ensure consistent assessment of third-party risk
- Developing more advanced proactive detection capability, including threat hunting and deeper analysis of security events
- Continuing to strengthen identity and access management, particularly in relation to authentication controls

It is important to emphasise that these areas are already being actively progressed as part of the ongoing CAF programme over the next 12 months. Given the scale and detail of CAF, it is expected that achieving a fully evidenced and validated position will take time. The current programme is therefore focused on progressive refinement, validation and improvement, rather than a one-off assessment.

## **8. Overall Assessment**

The College is at an early but well-developed stage in its formal alignment with the NCSC Cyber Assessment Framework.

The initial detailed assessment using CAF demonstrates that many of the required controls and governance arrangements are already in place. At the same time, it highlights areas where further work is required to ensure consistent, evidence-based alignment with CAF outcomes.

When considered alongside existing sources of assurance, including internal audit, Cyber Essentials certification and sector benchmarking, the evidence indicates that the College has a reasonably strong cyber security posture.

The next phase of CAF alignment will focus on moving from a strong controls-based posture to a more intelligence-led and proactive cyber resilience model, particularly in relation to threat understanding and detection capability.

## **9. Conclusion**

The College has made a strong start in assessing and progressing its alignment with the NCSC Cyber Assessment Framework.

The structured assessment using CAF, supported by HEFESTIS, provides a robust basis for understanding current maturity and identifying areas for improvement. This work will continue over the next 12 months as the College develops a more detailed and validated position.

In parallel, existing assurance mechanisms demonstrate that the College is already operating from a position of relative strength in cyber security. Cyber risk is being actively managed and a structured, evidence-based programme is in place to further strengthen the College's alignment with national best practice.