RM Cyber Essentials
Consultancy case study

# Using RM's Cyber Essentials consultancy to boost cyber security - one trust's story

## The client:

A multi-academy trust of approximately 30 primary schools in the south of England, the Midlands and East Anglia. RM has been the trust's IT managed service partner for a number of years.

## The challenge:

The trust is working on a digital transformation programme. This process involves standardising the operating model for its central functions, and the trust's IT team knew it needed to address cyber security.

The trust leadership and trustees shared this view. Everyone wanted to reduce the likelihood of a cyber attack disrupting their central operations. The trust's culture avoids a high level of prescription from the centre, which must be balanced against an appropriate level of cyber security provision.

> **"We knew that there was a lot that we didn't know. It was about identifying the major risks and starting to plug them as quickly as possible."**
>
> **Trust Programme Director**

In addition, the trust wanted to prepare for future audits and meet the Department for Education's Risk Protection Arrangement requirements.

The trust's IT team decided on Cyber Essentials as a benchmark for their central operation's cyber security position. The trust understood that it was unlikely to meet the scheme's requirements as things stood. Without the internal resources to identify where it would fall short and how to close the inevitable gaps, the trust engaged RM's Cyber Essentials Consultancy service to help.

> **"I wanted that prioritised list of actions to take away and do the work on. I wanted [the consultant] to shine a light on some of the practices we've got to give me the mandate to drive change organisationally."**
>
> **Trust Programme Director**

## The solution:

During RM's Cyber Essentials Consultancy process, one of RM's cyber security experts works with the client to create a holistic view of an organisation's Cyber Essentials readiness. The client receives a comprehensive report with recommended steps to take. The process also delivers a toolkit to help the client achieve compliance.

The project runs to an agreed schedule to maintain the right level of focus and prioritisation. In this case, the process took approximately eight weeks, including a break for the Christmas holiday period.

> **"It felt very collaborative. It felt very driven by our needs. It felt very personal, but it also felt that we were getting a significant level of expertise."**
>
> **Trust Programme Director**

### Stages of the process

- The trust started with a self-assessment according to a format provided by RM. This established a baseline for tracking progress.
- Consultant conducted a gap analysis based on the information provided by the trust.
- Consultant created an action plan and agreed the actions with trust stakeholders.
- Regular meetings between consultant and trust held to review progress and provide direction and support. During this period, the trust completed some of the identified actions using resources provided by RM.
- Consultant delivered the final report with a list of completed actions plus those still outstanding, ranked according to their respective importance.

### Achieving the trust's goals

RM's Cyber Essentials Consultancy is an iterative process. The output specification can be agreed upon as the project develops. In this case, RM provided tools such as policies and processes during the project so the trust could make improvements quickly.

RM's consultant engaged with different levels within the trust's central team to deliver a beneficial outcome. This helped the various stakeholders understand that everyone has a role to play in cyber security and that the resultant actions would align with the trust's culture.

Successful consultancy activities depend on partnerships. Relevant stakeholders in the trust's central team contributed fully to the process by sticking to the agreed timescale and being fully transparent during the information gathering stage.

## The outcome:

Following the project's completion, the trust understands its cyber security risks more fully. Using tools provided by RM, the trust has already eliminated some existing vulnerabilities found during the process.

The findings published in the report have given the trust a list of topics to address, with clearly defined actions and owners. To help complete these actions, RM provided tools including policy templates and process guidance.

Having spoken to the RM consultant during the project, the trust's senior leadership team now understands that cyber security is an ongoing process.

The scope of the consultancy project was to determine how likely the trust's central operations were to comply with Cyber Essentials. However, additional vulnerabilities emerged, and the final report listed them and provided suggestions for addressing them.

> "We now understand the risk much better than we did before. We've closed the open gates by tightening up some of the policies around how things work."
>
> **Trust Programme Director**

As the trust implements the report's recommendations, it improves its cyber security position and reduces its overall risk.

> "We're becoming incrementally safer by following the road map that we jointly developed with the RM consultant. In terms of the big corporate risk and the infrastructure to deal with that, it's given us a really good toolkit."
>
> **Trust Programme Director**

### Where the trust is now and where it's going

- By methodically approaching the thorny problem of cyber security, the trust feels more confident about its position.
- While no one can afford to be complacent about cyber security, the trust is at the forefront of taking a proactive approach.
- Multi-academy trusts put great stock in their culture and approach to managing their group of schools. Cyber security requirements can clash with the desire to take a less centralised approach. By acting on its security posture before an incident occurs, this trust can strike the right balance between its culture and adopting sufficiently robust policies that protect staff, pupils and the overall organisation.
- The trust has a baseline and approach to use when assessing the Cyber Essentials compliance of individual schools and managing cyber security processes with them.

> "The development for us of the tooling and the prioritisation was significant. And as a result, I think the corporate gap in terms of cyber risk has closed quite significantly."
>
> **Trust Programme Director**