To whom it may concern,

In consultation with Cyber Ireland, we would like to share our experience in the Netherlands by sending our submission for the National Cyber Security Strategy MTR Consultation below. If more information is needed, please feel free to contact us.

Trustmark for business to consumer web applications
Since online shopping has become more common and will continue to increase over the next few years, we need a way to ensure consumers know which websites are safe to shop and which are not. One way to do this is to introduce a trustmark.

Security trustmark
A secure trustmark logo can be displayed on business-to-consumer websites/webshops after undergoing a certification process to check whether they meet strict security requirements. The trustmark is a logo that is easily recognisable for consumers and ensures consumers of a reliable online retailer.

How to execute
A non-profit organisation could be put in place to manage a certification process. Any company can apply to become a member. A fee per web application should cover all expenses. Compliance with mandatory security checks (listed below) will result in a certification. The recertification process is needed every year to ensure compliance.

A marketing campaign is needed to create a general awareness of the trustmark. Similar trustmarks are already in place in the Netherlands (Thuiswinkel) and in Belgium (BeCommerce), where 92% of online shoppers know those trustmarks ensure a safe website. There, consumers actively look for the trustmark logo before making an online purchase.

Security Requirements
Legal, financial and/or technical checks should be done by carefully selected partners, supported by general rules and regulations.

- Check of general requirements with regard to rules and regulations
  - Retailer's trustworthy contact and location details
  - Clear offering, order process, and pricing
  - Secure payment environment (HTTPS)
  - A 14-day cooling-off period (minimum)
  - Buy now, pay later option
  - Sound complaint mediation and an independent arbitration committee
- A legal review focuses on GDPR with a valid privacy and cookie statement on the website.
- Financial monitoring assesses whether the online retailer is financially healthy enough to fulfil their obligations to consumers.
- A technical check focuses on cyber security and consists of a very thorough vulnerability scan of the web application. Vulnerabilities according to the OWASP Top10 are checked, and any high risks found need to be fixed. A safe result is mandatory for the certification.

Met vriendelijke groet | Kind regards,