Design safe and more resilient software applications

Building effective digital trust for your software applications

Your partner
in progress

In our digital and connected world, we conduct transactions and access our personal and financial information online. Increasingly, we do this using web and mobile software applications (apps) on a variety of platforms and devices.

In 2022, apps on smartphones and tablets were used by 42.5 million adults (94% of the online adult population) in the UK.[1] In 2023, apps were downloaded 2.3 billion times in the UK alone.[2]

Ongoing developments in digital technology mean both end users and businesses continually face new risks. To protect users' personal and financial data, and businesses' reputations, these risks must be addressed.

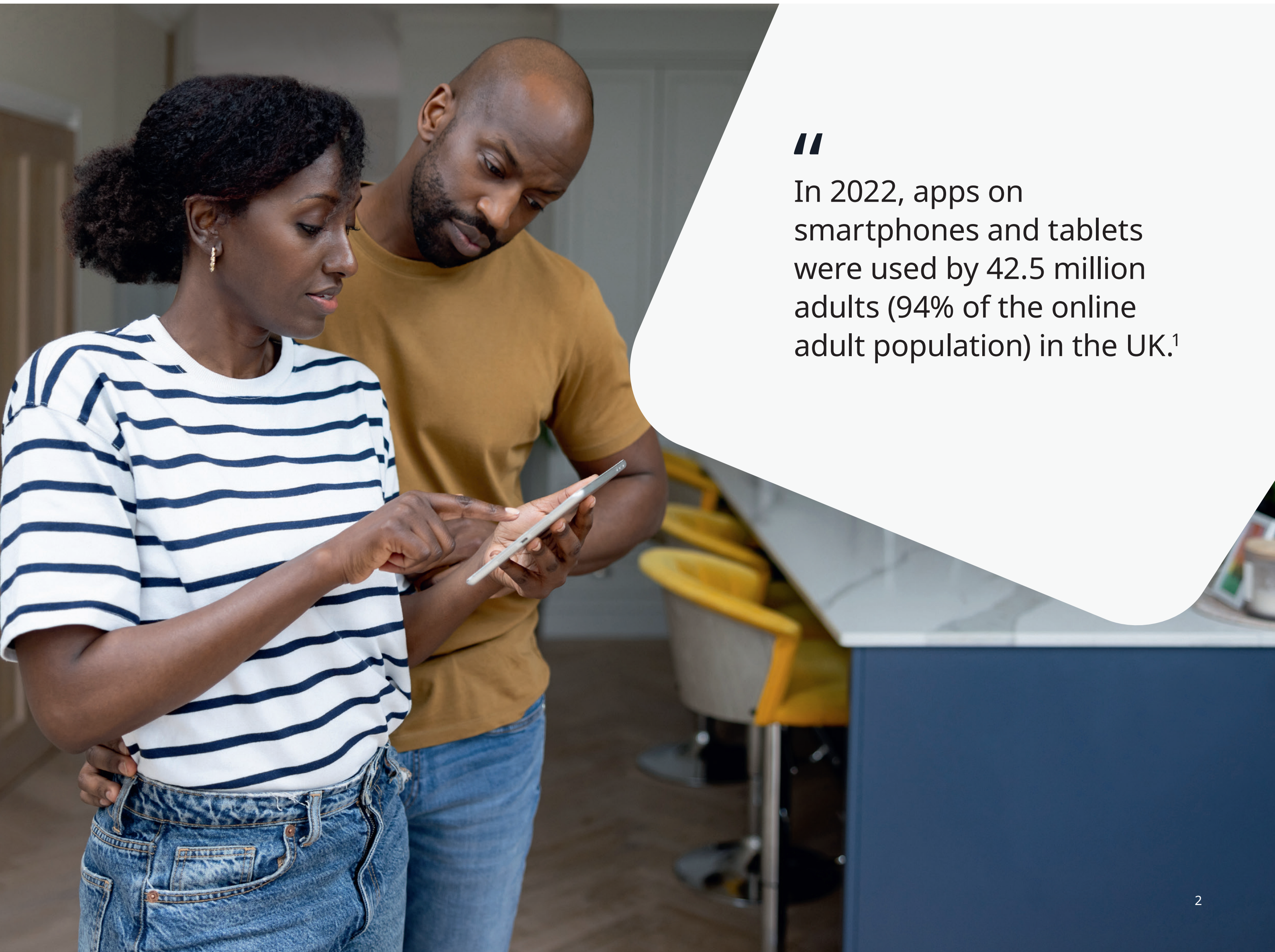
Software apps face many security risks such as injection, logic and design flaws to authentication and authorization flaws, plus attacks on software supply chain that can compromise functionality, performance, and reliability, as well as the privacy of the data that these apps handle.

Addressing the challenges

Independent testing and certification of software apps against best practice specifications is a key activity. Not only will this ensure applications are up to date with the security controls they have in place, they will also be in a better position to address the latest cyber threats and vulnerabilities as they arise.

Applications and the security landscape are very dynamic by nature. Therefore, regular testing and certification activities in line with security standards are essential to keeping users safe on an ongoing basis.

Through our third party testing and certification activities, based on the Open Web Application Security Project (OWASP) standards, we can help software developers to address these challenges.



> "In 2022, apps on smartphones and tablets were used by 42.5 million adults (94% of the online adult population) in the UK.[1]

What is OWASP?

OWASP is a non-profit foundation that works to improve software security worldwide. It’s dedicated to making application security visible so individuals and organizations can make informed decisions about security risks.

OWASP has developed a number of standards that define application security requirements or tests that architects, developers, testers, and security professionals can use to define, build, test, and verify secure applications.

The OWASP standards

OWASP is a non-profit foundation that works to improve software security worldwide. It’s dedicated to making application security visible so individuals and organizations can make informed decisions about security risks.

OWASP has developed a number of standards that define application security requirements or tests that architects, developers, testers, and security professionals can use to define, build, test, and verify secure applications.

OWASP (ASVS) Web Applications

For web applications, OWASP has developed the Application Security Verification Standard **(OWASP ASVS).**

The OWASP Application Security Verification Standard (ASVS) project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

OWASP (MASVS) Mobile Applications

For mobile applications, OWASP has developed the Mobile Application Security Verification Standard **(OWASP MASVS).**

To ensure Google Android and Apple iOS mobile apps are secure and meet industry-standard security requirements, regardless of development approach.

OWASP MASVS testing follows the Mobile Application Security Testing Guide (MASTG), a comprehensive manual for mobile app security testing and reverse engineering.

The OWASP MASVS and MASTG are trusted by the following platform providers and standardization, governmental and educational institutions.

CREST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ioXt
internet of secure things

android

These OWASP standards are living documents, regularly updated to reflect the changing threat landscape and new attack vectors.

OWASP security levels

The OWASP ASVS and MASVS standards define three security verification levels.

OWASP	ASVS
Level 1	Low assurance (foundational).
Level 2	Applications that contain sensitive data, which requires protection. This is the recommended level for most software apps.
Level 3	Most critical applications that perform high-value transactions, contain sensitive medical data, or any application that requires the highest level of trust.

OWASP	MASVS
Level 1 (Essential)	Provides a baseline for the most fundamental security requirements and best practices that every mobile app should meet to protect against common threats.
Level 2 (Advanced)	Additional security measures and best practices for mobile apps to address advanced threats.
+R (Resilient Security)	For applications that have a strong need to safeguard their own business assets and logic.

OWASP security testing categories

ASVS security testing categories (14 areas)

- Architecture
- Authentication
- Session Management
- Access Control
- Input Validation
- Stored Cryptography
- Error Handling and Logging
- Data Protection
- Communication Security
- Malicious Code
- Business Logic
- Files and Resources
- Web Service
- Configuration

MASVS security testing categories (8 areas)

- MASVS-STORAGE: Secure storage of sensitive data on a device (data-at-rest).
- MASVS-CRYPTO: Cryptographic functionality used to protect sensitive data.
- MASVS-AUTH: Authentication and authorization mechanisms used by the mobile app.
- MASVS-NETWORK: Secure network communication between the mobile app and remote endpoints (data-in-transit).
- MASVS-PLATFORM: Secure interaction with the underlying mobile platform and other installed apps.
- MASVS-CODE: Security best practices for data processing and keeping the app up to date.
- MASVS-RESILIENCE: Resilience to reverse engineering and tampering attempts.
- MASVS-PRIVACY: Privacy controls to protect user privacy.

Cybersecurity testing and certification services for software applications

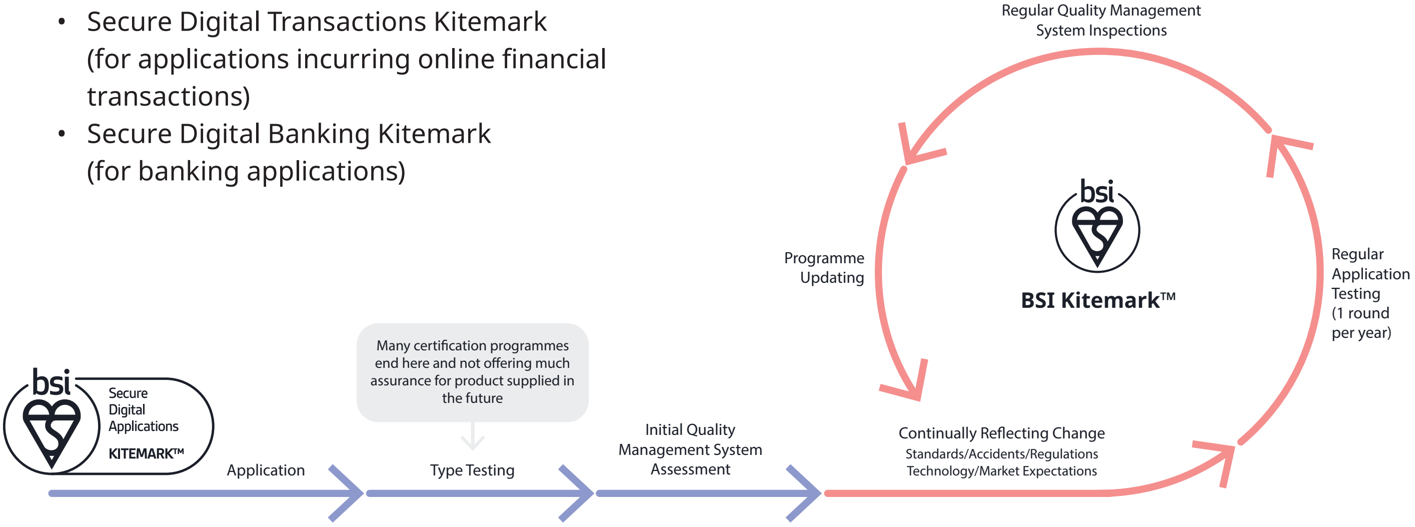
Give customers the reassurance they are looking for that their app is secure by having it independently tested and certified.

We help software developers achieve this goal through:

- Third-party testing (one-off) and the issue of Certification of Conformity (1-year validity) according to the latest OWASP ASVS and OWASP MASVS (following OWASP MASTG) standards available.
- Secure Digital Application Kitemark testing and certification services, including:
  - Secure Digital Applications Kitemark (for most software applications)
  - Secure Digital Transactions Kitemark (for applications incurring online financial transactions)
  - Secure Digital Banking Kitemark (for banking applications)

Initial third-party testing according to OWASP standards is a great first step towards building credibility with customers and app users. It could also be the first step towards achieving the BSI Secure Digital Applications Kitemark. In addition to app testing, the BSI Kitemark certification process also requires third party auditing of the Quality Management System for app development and maintenance, to ensure that compliance and security control remains at the heart of the app development lifecycle.

A requirement of the Kitemark certification programme is the annual testing of software apps and regular Quality Management System audits, to verify that security integrity has not been affected by changes to the app, the threat landscape and new attack vectors.



Secure Digital Applications KITEMARK™
Application
Many certification programmes end here and not offering much assurance for product supplied in the future
Type Testing
Initial Quality Management System Assessment
Continually Reflecting Change
Standards/Accidents/Regulations
Technology/Market Expectations
Regular Application Testing (1 round per year)
Regular Quality Management System Inspections
Programme Updating
BSI Kitemark™

Applicable levels for these Secure Digital Applications

ASVS	SDA	SDT	SDB
Level 1	✓	X	X
Level 2	✓	✓	✓
Level 3	✓	✓	✓

MASVS	SDA	SDT	SDB
Level 1	✓	X	X
Level 1+R	✓	X	X
Level 2	✓	✓	X
Level 2+R	✓	✓	✓

We test and certify the following types of software applications

Apps are a great way for almost all sectors to engage with final users and create personalised experiences for their customers. A trusted app can help build loyalty, brand awareness and increased added value. Apps also offer convenience of access; whether at work, at home or on holiday, users can check information, update details, place orders, play games and more.

Main sectors:
- Financial online services
- Medical applications
- Health and Fitness
- Utilities
- Manufacturing
- Sustainability
- Gaming
- Banking (online / mobile)
- Social networks
- Shopping
- And more

Benefits of testing and certification

In an industry that is yet to be regulated, it’s important to be able to reassure customers and end users that their app – and data – is secure. Demonstrate commitment to app security by working towards recognized standards and undertaking third-party testing of software applications with a reputable organization. Provide your clients and end users peace of mind, and gain an all-important competitive edge.

For businesses:
- Independent validation of your digital security
- Enhance your cybersecurity leadership
- Differentiate your service
- Increase trust in your brand
- Enhance your reputation
- Attract new customers
- Stand out from your competitors
- Identify areas for security improvement

For end users:
- Easy identification of websites and apps they can trust with their personal details
- Easy identification of banks and other financial providers with trusted digital security
- Greater confidence when buying online
- Increased trust in websites and apps

Why BSI?

We have been working with app developers for over five years, delivering over 100 projects. Our highly skilled engineers and CREST-qualified testers work with you to ensure your app is secure and conforms to the industry's most recognized standards. Not only are we an experienced testing body, we have been certifying products for over 120 years, adapting and changing our services to suit our times.

At BSI, we focus on delivering testing and certification services underpinned by quality, safety, reliability, and trust. As a global organization, we have the scale and reach to support any size of organization and in our dedicated state-of-the-art IoT laboratory, where our experts provide fast and effective testing for a wide range of IoT products.

BSI has a world-class cybersecurity capability recognized by UKAS accreditation, CREST global accreditation, National Cyber Security Centre, and IoT Security Foundation combined with decades of experience in product assurance, testing and certification.

Discover more at
bsigroup.com

Your partner
in progress

BSI Kitemark™ certification for Secure Digital Applications

Discover more at:
page.bsigroup.com/securedigitalapplicationskitemark

References

1 Baker, N., 2024. UK mobile phone statistics. uSwitch. (online) 7 February. Available at: https://www.uswitch.com/mobiles/studies/mobile-statistics/ (Accessed 20 May 2024).

2 Wylie, L. (2024) 'UK App Market Statistics (2024)', Business of Apps, 1 February. Available at: https://www.businessofapps.com/data/uk-app-market/ (Accessed: 20 May 2024).