Vulnerability Testing
For Financial Services

Helping you to understand how criminals view your organisation

AJC and We Fight Fraud (WFF) work together in partnership to offer a tailored end-to-end fraud prevention solution for organisations to address the challenge of the ever-evolving fraud landscape. Our approach encompasses market-leading vulnerability testing and proactive strategies to bolster corporate resilience. Clients will have access to a team of 40 specialists with extensive knowledge and experience, dedicated to identifying, understanding, and mitigating threats to your organisation.

Our holistic strategy begins with vulnerability testing conducted by WFF to assess the latest attack techniques. We then analyse the results alongside cutting-edge research, providing comprehensive fraud prevention training and offering a mitigation solution programme to enhance corporate resilience, complete with ongoing audits and reviews.

Identify
How you might be targeted by criminals or malicious attackers

→

Understand
What could happen if they did gain access to your business

→

Mitigate
Most importantly; how you can stop them in the future.

We can help you assess your fraud risks enabling you to make good business decisions.

Vulnerability Testing

Strategic Corporate Resilience

Vulnerability testing is critical to your Strategic Corporate Data Resilience and Governance Planning. Data is the new cash, and bad actors will use every vulnerability to compromise the data you hold or manipulate and exploit compromised data within your systems. Allow us to help you stay ahead of criminal activity and protect your clients data and your organisation.

By combining multiple perspectives, integrated teams become more than a sum of the parts. This goes for penetration testing, red teaming and human hacking. Our testing examines your organisation, products, processes and customers through the eyes of a criminal. We identify key vulnerabilities, revealing the attack vectors bad actors will use to damage your organisation.
We then provide solutions and governance that ensure any vulnerabilities are managed and your organisation stays protected.

Your organisation is best placed to identify strategic areas for concern that you wish us to address. At the start of the test period, an initial strategic planning meeting will offer the opportunity to raise any specific areas of concern that have yet to be discussed. It will also set the parameters for the test.

Oversight & Compliance

At the start of this test, we ask that you assign a designated officer to communicate with us about the project as a single point of contact. Our testing then takes a staged approach.

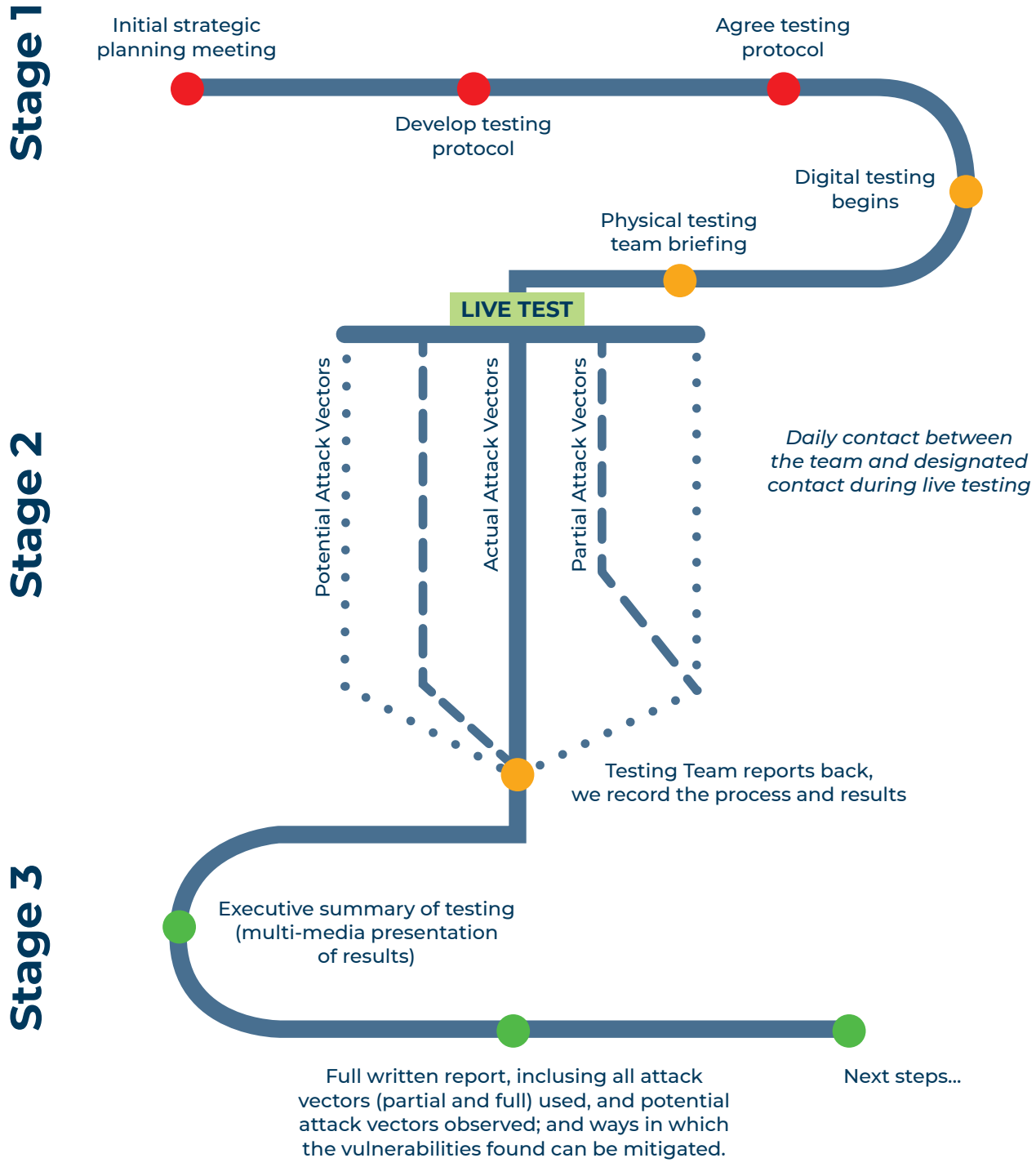
Stage 1 is the planning stage where we work with you to target the areas of business you are most concerned about. Here we set the parameters of the test. This may be setting an objective to be achieved or setting time constraints on the testing team.

Stage 2 is where we go into testing the people, processes, products or procedures defined in stage 1. We will attempt a number of attack vectors including digital and cyber attack, physical and social engineering (where appropriate).

Stage 3 is where the governance team takes over, providing a full report both written and audio visually to your organisation (usually the single point of contact and the c-suite). Options for remediation are presented here in an easy to understand report that highlights examples of good practice as well as key priorities for improvement in order to build your corporate resilience.

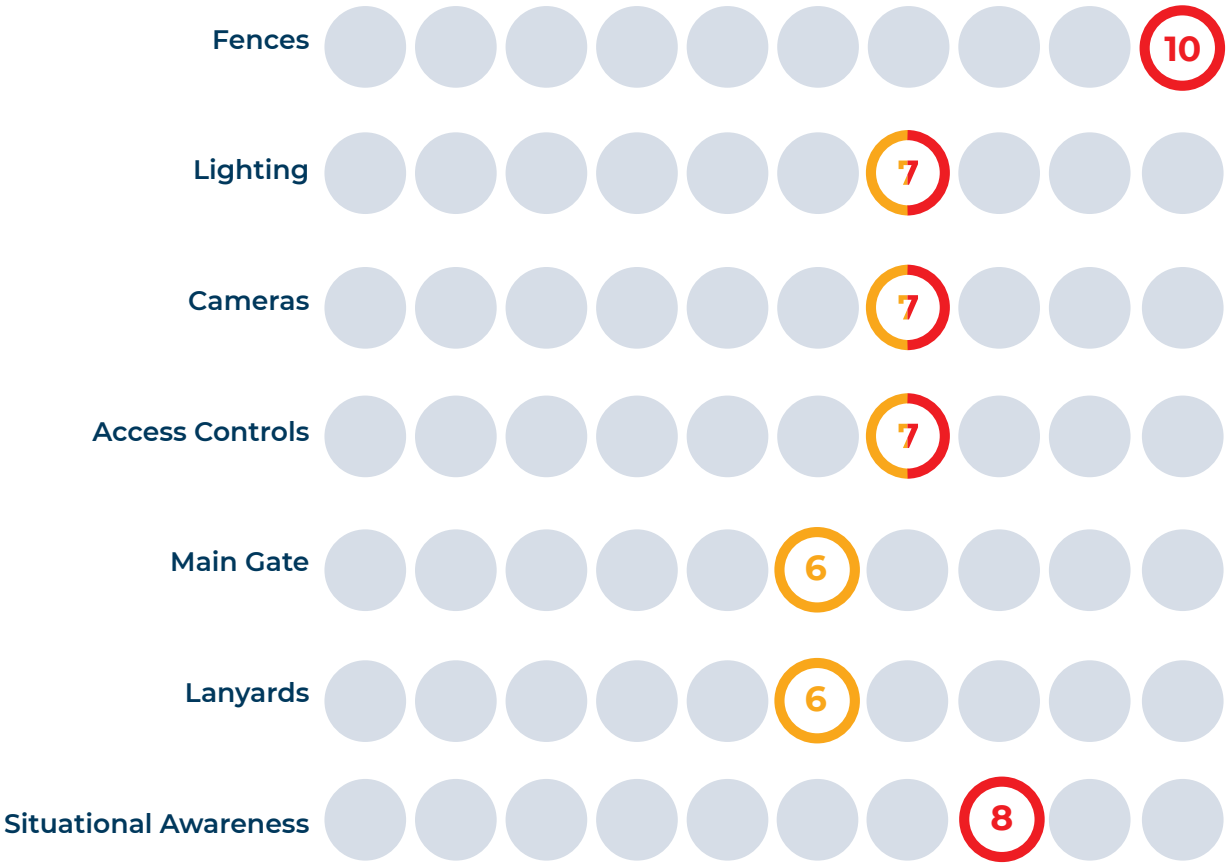
Using this approach, testing can be paused if necessary, when vulnerabilities are found and communicated to your designated officer. This allows all our testing to be responsive to not only identifying criminal opportunities but also the needs of your organisation in deciding how to respond to any vulnerabilities found.

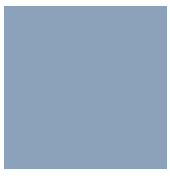
The Testing Process



Reporting

At the end of the test you will receive a full report for the project, which will include the method of testing, the attack vectors identified, and our recommendations for reducing, managing, or eliminating the vulnerabilities detected. This report is presented as a written dossier and a presentation that includes audio/visual evidence directly from testing with detailed, at a glance, risk-scores.





Verbal and email communication with AJC on every live test day and at agreed milestones.

Briefing from the team (presentation with audio visual elements demonstrating findings of the test).

Full written reports, detailing attack vectors (evidenced and observed) and ways to mitigate the threat.

Mitigation

AJC will help remedy the vulnerabilities found within the Testing process.

As our testing shows, the Global environment continues to change rapidly, requiring companies to be nimble and understand Internal and External threats to their organisation. AJC prides itself in delivering robust solutions to identify and manage these threats.

We have a proven track record of breaking down the requirements, identifying the solutions, and implementing programmes to meet a variety of regulations and manage fraud within the appetite of the organisation.

Engagements can either be bespoke or formulaic (based on regulation/standards), driven by the customer demand.

Typical engagements include:

- Strategy review
- AML/Fraud
- VISA GARS Review
- VISA Merchant Risk Review
- Cyber/information security
- SWIFT CSP Audit
- Policy frameworks
- Business continuity
- Risk management
- Data protection
- BREXIT
- International standards
- Vendor management frameworks
- Assurance reviews
- Training
- Data Protection Officer
- Chief Information Security Officer

AJC are on a number of approved third party and auditor lists, including those maintained by VISA and SWIFT. They are the chosen partner of Bottomline for the delivery of independent SWIFT CSP Audits.

Mitigation

Client Case Study

Client: A global specialist investment company.
Project: To test the physical security of the UK Head Office.

Identified Attack Vectors

The physical team were able to access and compromise the RFID entry control system on a service entrance to the building in order to collect access card data.

This enabled the team to create clones of the access card data collected. One of the cards cloned was a master security pass which acted as a master key - giving the team access to all areas of the building.

Using open source intelligence gathered by the digital team about the senior leadership and C-suite, the physical testing team gained entry through the front door by socially engineering security guards at reception, and other members of staff on the target floor.

The access gained demonstrated how the physical team could access the boardroom to plant listening devices in order to conduct corporate espionage or gain access to key digital assets in order to steal data.

Implications and Risk

The company was in danger of a major data breach. By gaining access to the building in multiple ways, the team could have planted listening devices and harvested data in an act of corporate espionage or, due to the nature of some contracts, a terrorist attack.

Solutions

Our team provided a thorough report to the client for them to ensure that the vulnerability was addressed with the third party that provided external security with practical options for resolution.

A suite of training modules was developed for managers and all customer-facing staff to enhance their awareness of risks from social engineering and how to deal with them. Advice was also given to C-suite about personal privacy and OSINT vulnerabilities.

Return On Your Investment

We have a track record of discovering systems, processes, and human vulnerabilities. These could have cost our clients billions of pounds in losses, as well as significant reputational damage, and result in a significant loss in stakeholder confidence.

Our clients - having taken the decision to engage our end to end vulnerability assessment and remediation service - have benefited from:

> Continual monitoring of the dark web and criminal networks for 'noise' / 'adverse media' or intelligence about threats to their organisation.

> Targeted testing, tailored to ensure the most pressing issues for that organisation are examined first.

> The opportunity to test new products and services before they go 'live' to their clients and the inclusion of AJC's insights into new product design.

> An in-depth, evidence-based, understanding of how the risks identified might impact their firm and its various stakeholders.

> Practical steps and support to help them to manage and mitigate the various risks. Including the option of bespoke training to address specific human vulnerabilities.

Contact us today

AJC
T 044 (0)20 7101 4861
E info@ajollyconsulting.co.uk
www.ajollyconsulting.co.uk

WFF
T 044 (0)20 3633 0996
E contact@wefightfraud.org
www.wefightfraud.org

We know that the potential cost of fraud to your business can extend beyond your bottom line, it can impact your people, culture and ultimately your reputation.

AJC together with WFF are here to support you.