



**risk  
CREW**



# SECURITY TESTING SERVICES

Discover the effectiveness  
of your security systems



# STAY AHEAD OF THREATS WITH EFFECTIVE TESTING



As the security threat landscape is constantly changing, it creates many challenges for organisations to stay on top of threats to information systems and assets.

**Our expert penetration testing engineers can help you stay ahead of security threats.** The Risk Crew team is comprised of expert security engineers who use best-practice security assessment methodologies and unmatched analysis capabilities to help you understand the effectiveness of your organisation's security operation.

## Risk Crew's Unmatched Deliverables

Our team provides a comprehensive service which includes a detailed report, courtesy workshop, retesting and on-call assistance – all backed by a 100% satisfaction guarantee.

### Courtesy Workshop

The report is presented in a workshop with applicable business stakeholders to ensure their understanding of the findings and the risks associated with hosting the business information assets on the platform.

### On-call Advice Assistance

We provide advice and assistance for 30 days following the report submittal and answer any questions that arise from implementing remedial actions and ensuring risk reduction.

### Detailed Report

The report details specific vulnerabilities identified on the platform, how they were identified, methods and tools used to identify them and visual evidence if applicable. The report shall indicate a security vulnerability risk rating for risk reduction references.

### Complimentary Retesting

We offer retesting to verify remedial actions were effective. Upon completion, we'll provide you with a summary report verifying remedial measures have been implemented.

### Customer Promise

Risk Crew provides an unparalleled penetration testing solution covered by a 100% satisfaction guarantee.

# Security Testing Services

Risk Crew provides a range of security testing includes:



## Network Security Penetration Testing

These tests will evaluate the effectiveness of your network security by simulating an attack from a threat agent. Testing is scoped to meet your specific business or compliance requirements, and can be conducted via the external network, having no previous knowledge of your infrastructure or by conducting an internal penetration test of your systems, servers and workstations.



## Web Application Security Penetration Testing

Verify the security integrity of your web applications with testing that identifies exploitable vulnerabilities associated with your website to ensure the security integrity of its transactions. Testing includes the design and delivery of a granular review of the target application to identify all associated vulnerabilities and manual testing of those vulnerabilities to determine the extent to which they can be exploited and their impact on the security integrity of the application.



## Mobile Device Security Testing

Identify vulnerabilities associated with the portable devices used to access your sensitive information assets. Our engineers will test client-side and server-side, review device hardware, operating system and applications for existing security vulnerabilities that if exploited, could potentially allow unauthorised access.



## IoT Security Penetration Testing

Tests provide an investigative process designed to assess the attack vectors associated with your IP-enabled business devices. The objective is to assess the capability of existing security controls to identify and prevent an IoT related breach. Risk Crew can test built in-house or third-party devices.



## Mobile App Security Testing

Assess the security integrity of applications that run on mobile device platforms and operating systems. This service will identify security vulnerabilities which could be exploited to compromise the device and the data it may process, store, or transmit.



## Cloud Security Assessments

This service will identify potential security vulnerabilities associated with your cloud service for remediation or risk acceptance. Our effective cloud security testing benchmarks the security configuration of your hosting environment.



## Security Vulnerability Testing

Tests provide a cost-effective way of identifying weaknesses in systems and applications that process, store and transmit your information assets. Risk Crew leverages automation through vulnerability scanners to identify common configuration and patch issues.



## Social Engineering Testing

Detect weaknesses in operational and business processes which could be exploited for unauthorized access and get invaluable insight into the genuine level of security your information security risk management programme provides with Social Engineering Testing.



## APT Testing

Advanced Persistent Threat testing is comprised of a customised campaign of multi-vector simulated attacks designed to assess your capability to defend against threat. Our comprehensive testing will confirm whether your defences can detect and deter this severe threat.



## Red Team Testing

Verify the security controls you've implemented in your people, processes and technologies by pitting them against real-life cyber-attacks. Attacks are specifically designed to validate the effectiveness of your incident identification and response practices; giving you a hacker's view of your information and cyber security defence posture.







## Risk-Driven Application Security Testing

Ensure the security integrity of business-critical applications prior to launch. This innovative service is comprised of four activities: identifying application design flaws, threat & risk assessment, threat & attack modeling and risk-driven penetration test.

# WHY CHOOSE RISK CREW

When you choose Risk Crew, you're electing to work with qualified experts.

Our experienced security engineers implement detailed testing methodologies using proprietary and open-source tools ensuring they can effectively assess your business's capabilities to detect and mitigate attacks against your business systems. All engineers are thoroughly vetted and subject to in-depth professional, criminal and credit records checks.

-  **Best Practice**  
Risk Crew follows best practices including OWASP and NIST
-  **Accredited**  
Engineers carry CREST, C√SS, C|EH and GIAC credentials
-  **Certified**  
Engineers hold ISACA CISSP, CISM and CRISC certifications
-  **Subject Matter Experts**  
Risk Crew engineers are SMEs with published articles in industry journals & magazines

## Our Credentials



# TESTING METHODOLOGY

Our step-by-step methodology is simple and effective.

## 1. Reconnaissance

Reconnaissance is the process of collecting various information about the target (application) in order to assist exploitation. The objective of this process is to gather intelligence on how the target organisation operates, its security postures i.e. how the website has been developed, how often it is updated and, potentially, how the organisation can be attacked.

## 2. Access Control

The objective of access control testing is to examine the quality, resilience and strength of various aspects within the target application. Various manual testing scenarios will be deployed to ensure that access control mechanisms respond and function securely and appropriately. We would typically test with & without user credentials.

## 3. Manual Exploitation

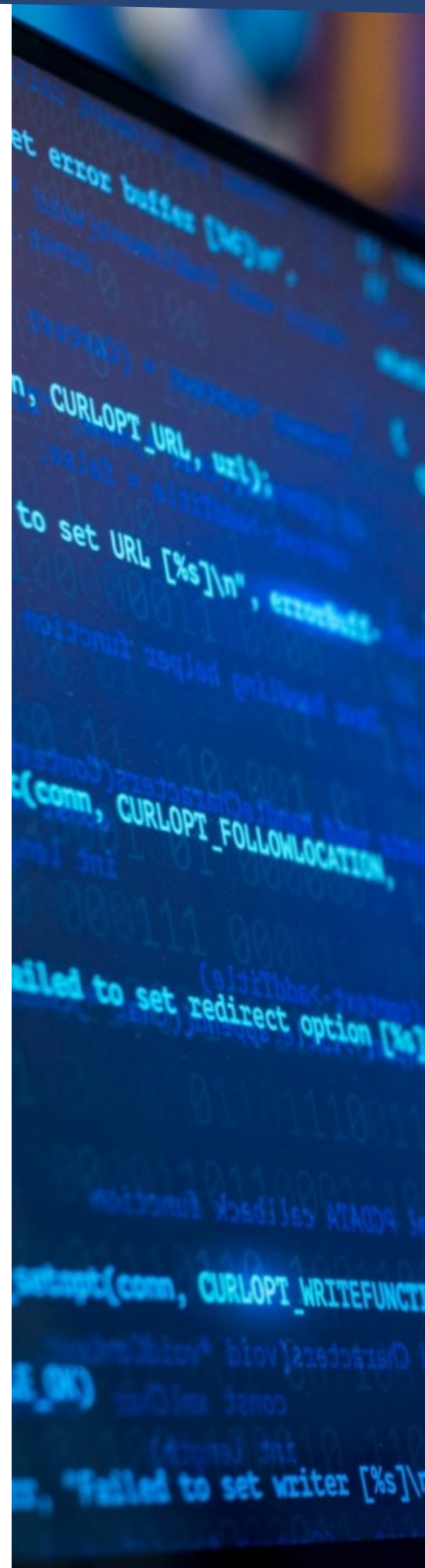
Using all the intelligence observed and gathered during the reconnaissance and access control testing activities, Risk Crew will deploy various methodologies that are appropriate to the target environment. The over- all objective of this phase is to attempt to exploit the vulnerabilities identified to obtain unauthorised access or permissions and verify the security integrity of the target environment. This is the critical component to the testing.

## 4. Reporting

Upon test completion, we'll draft a detailed report of our findings and recommendations. The report will be comprised of a "plain English" executive summary as well as a detailed technical description of each vulnerability identified, the associated risk level, visual evidence of its exploitation (where applicable) and step-by-step directions for its remediation.

## 5. Retesting

Once you have remediated any vulnerabilities identified in our testing, the service also includes "complimentary" re-testing to verify remedial actions were effective. Upon completion of the re-testing, we'll provide you a summary report verifying remedial measures have been implemented.



*Let our expert security testing engineers help you stay ahead of security threats.*

## About RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

## Contact us for more information



5 Maltings Place  
169 Tower Bridge Road  
London SE1 3JB  
United Kingdom



[information@riskcrew.com](mailto:information@riskcrew.com)



+44 (0) 20 3653 1234



[riskcrew.com](http://riskcrew.com)