

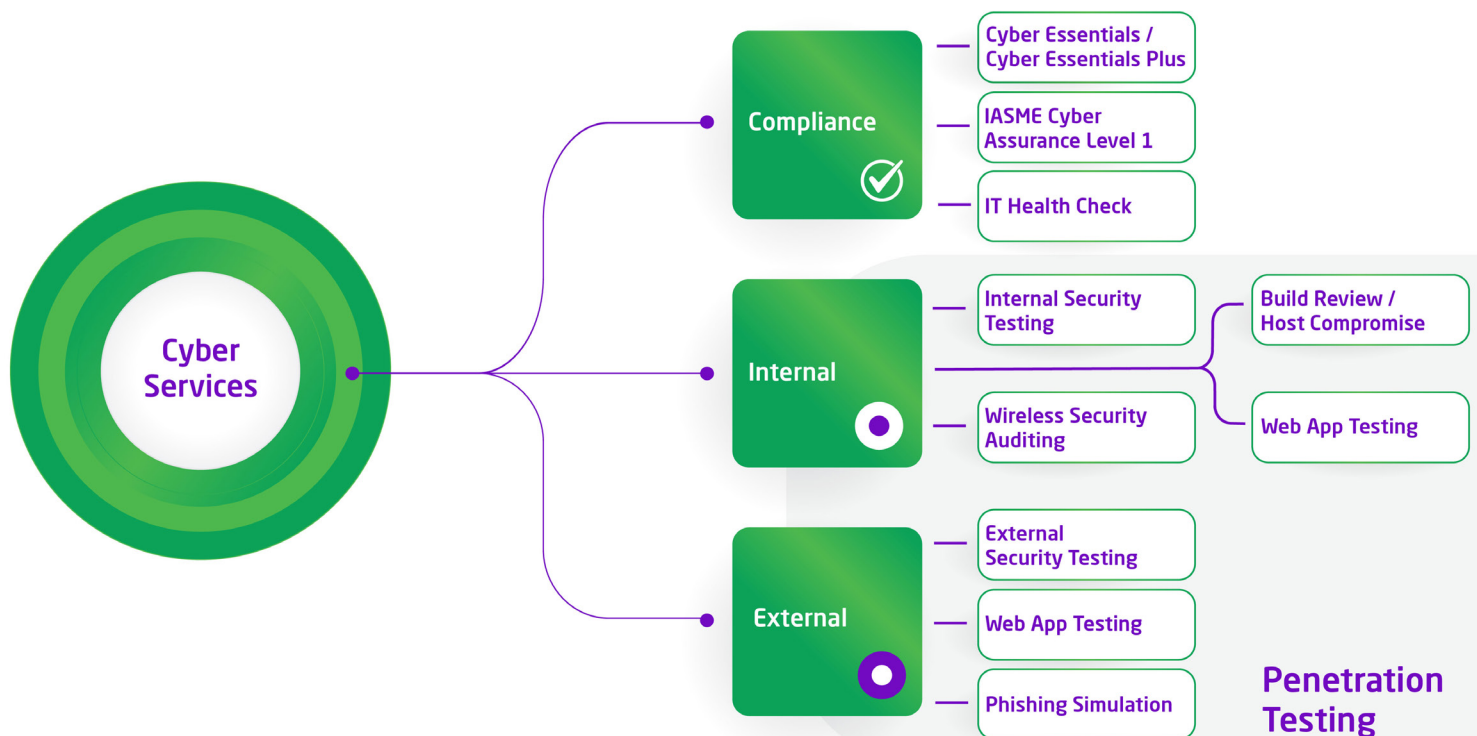
# Penetration testing

Identify, assess and prioritise organisational vulnerabilities






CNS, part of the Flow group, have a CREST approved cybersecurity team who will complete testing under real attack conditions replicating non-invasive hacker techniques. Any vulnerabilities identified are delivered through clear reporting with advice on how to remediate.

## Benefits of our penetration testing:

- Improve business awareness and understanding of your cybersecurity risk exposure
- Detect and remediate security threats before they can be exploited by cyber criminals
- Prioritise security investments based on actionable intelligence
- Protect company reputation whilst displaying your continuous commitment to security



## Flow's expert cyber services

The various subject areas of penetration testing			
	Subject area	What do we test?	What is the aim?
	Internal security testing	Internal network including servers, workstations, devices	To identify vulnerabilities which could be exploited by an attacker who has gained access to the internal network
	Wireless security auditing	Wireless networks	To identify vulnerabilities that could be exploited by an attacker who is attempting to gain unauthorised access to the network or to intercept sensitive information being transmitted over the network
	Host compromise simulation	Simulating a real-world attack on a host including server, workstation	To identify vulnerabilities that could be exploited by an attacker who has already gained access to the internal network
	External security testing	External-facing infrastructure including web applications, network perimeter, cloud services	To identify vulnerabilities that could be exploited by an attacker who is trying to gain unauthorised access to the organisation's network from the outside
	Web app testing	The security of web applications including online shopping carts, webmail applications, other web-based software	To identify vulnerabilities that could be exploited by an attacker who is attempting to gain unauthorised access to sensitive information or to take control of the application

