PROACT

G-Cloud 15

Operational Resilience Assessment

PROACT

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
04/12/2025	Colin Abram	V1	Document Upload

PROACT

Operational Resilience Assessment

Proact Operational Resilience Assessment service

Description

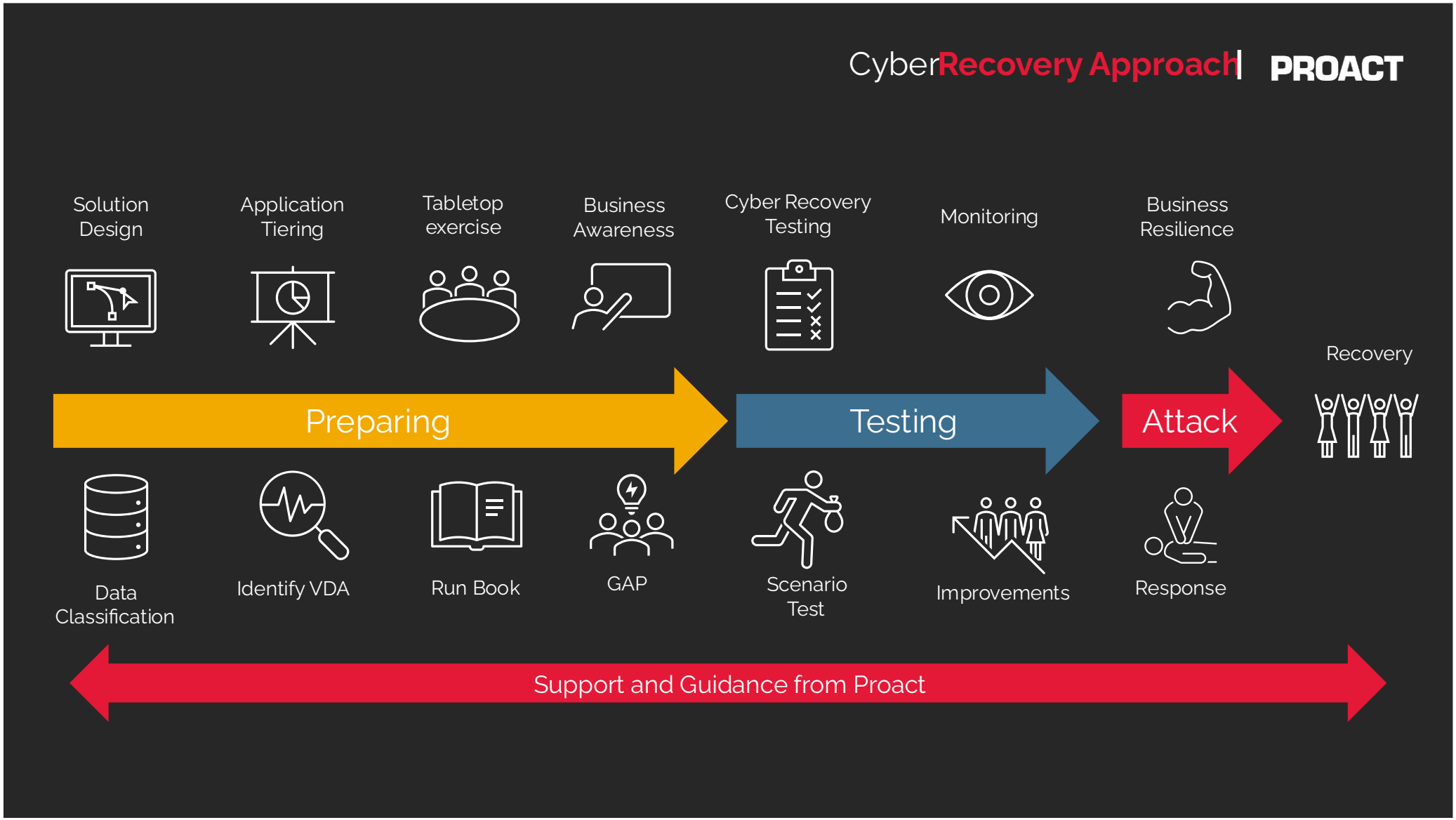
Proact IT UK Operational Resilience Assessment is a consultative service to help your company understand what their critical data assets are and what should be put into a Vaulted backup to assure the most testable, repeatable, and measurable recovery.
With Proacts guidance you will be able to understand where to start and how to achieve a Governance (NIS / NIS2 /Ops Res) Auditable process that is regularly tested.
Proact has many solutions that can be applied to your business, but the assessment is required to comprehend which is the correct service.

Features

- Proact Supports On-Prem, Co-Location and Public cloud applications of the service.
- Assessments to help your business understand your most Vital data assets.
- Solution design so the product will recover your business within your survival timeline.
- Application Tiering to help your recovery process streamlining.
- Run-Book creation.
- Business Awareness – So the whole business knows what to do during a ransom aware attack.
- Managed your isolated Cyber Recovery testing and collect Audible evidence of testing process
- Managed Scenario Cyber testing
- Response plans

Benefits

- Auditable testing managed and documented.
- Consultancy to make sure your business has a Rapid recovery with industry leading vendor.
- Simplification of the cyber recovery process
- Flexible and scalable
- Project planning
- Business awareness and support


CyberRecovery Approach
PROACT
Solution Design
Application Tiering
Tabletop exercise
Business Awareness
Cyber Recovery Testing
Monitoring
Business Resilience
Recovery
Preparing
Testing
Attack
Data Classification
Identify VDA
Run Book
GAP
Scenario Test
Improvements
Response
Support and Guidance from Proact

Proact Security Portfolio

PROACT

Identify	Vulnerability Management, Threat Intelligence, Attack Surface Monitoring
Protect	Firewalls, Endpoint Protection, Phishing Defences, Web Proxies, ZeroTrust Access, Authentication (MFA), Staff awareness, Cyber Training/Education
Detect	Security Logging and Detection / 24/7 SOC services
Respond	MDR/XDR Services, Containment, Eradication, Incident Response Planning and Execution
Recover	Cyber Recovery and Disaster Recovery

Pricing
Pricing for Cyber Ransomware Recovery Assessment services is charged based on Proact's day rates as detailed in the rate card below.

Professional Services Day Rates

Level	Strategy and architecture	Change and transformation	Development and implementation	Delivery and operation	People and skills	Relationships and engagement
1. Follow	N/A	N/A	£600	£600	N/A	N/A
2. Assist	N/A	N/A	£600	£600	N/A	N/A
3. Apply	N/A	N/A	£850	£850	£850	£850
4. Enable	£1,000	£1,000	£1,000	£1,000	£1,000	£1,000
5. Ensure, advise	£1,350	£1,350	£1,350	£1,350	£1,350	£1,350
6. Initiate, influence	£1,750	£1,750	£1,750	£1,750	£1,750	£1,750
7. Set strategy, inspire, mobilise	£2,000	£2,000	£2,000	£2,000	£2,000	£2,000

Pricing excludes VAT.

Pricing is for resource only and full day rates include travel and expenses within the UK, work outside the UK will be quoted separately to include travel and expenses costs.

Standard working hours are 09:00 to 17:30, Monday to Friday excluding UK public holidays – Uplift for out of hours: Evenings, Weekends and Bank Holidays x2.

Services are subject to scope of works definition – Some specific skills or to meet urgent timescales may require 3rd parties and may incur a higher cost, which will be quoted on a case-by-case basis.

The following table provides an overview of the deliverables provided against the day rate levels detailed above:

Level	Title	Description
3	Field Engineer	• Installation of pre-configured devices and associated connections. • Conducts basic hardware operational tests, troubleshoots malfunctions and replaces faulty hardware components, where applicable
4/5	Professional Services Engineer	• Experienced Technical Expert in their area of specialism • Defines the installation procedures and order of work • Installation of hardware and software • Conducts testing and recoding of results • Completes health checks and documents recommendations • Carries out fault diagnosis • Customer handover
6	Technical Architect	• Technical Lead providing expert technical knowledge in their area of specialism • Experienced in capturing requirements and translating into multi technology / multi-vendor designs • Capable of extrapolating the impact of Data Protection and Disaster recovery into architecture
7	Enterprise Architect	• Ability to design to business goals and systems requirements • Capable of running large multi-national programmes • Assistance in the development of IT Strategy, Policies and Governance • Able to write detailed Business Cases