Local Government Association

Bespoke Cyber Support for Councils

Gain advice and support to improve your cyber security culture

Local Government Association

Contents

01 The threat, our mission, and our offers

02 Common challenges for councils

03 Cyber Reaction Exercises

04 Testimonials and meet the team

Local Government Association

The cyber threat to local government

"The pandemic has also brought about an acceleration in digitisation, with businesses and **local government** increasingly moving services online [...] **This has broadened the surface area for attacks** and has often made cyber security more challenging for organisations."

NCSC Cyber Threat Report 2021

Our support offer vision

©nouveau.co.uk

Vision

- Councils have an improved understanding of cyber risk,
- they prevent and resist cyber attacks more effectively,
- and have the cyber security skills at every level to do so.

How we do this

The LGA's bespoke cyber support offer, the **Cyber 360** and **Cyber Reaction Exercises**, support councils to

- hear a different perspective on their cyber security culture
- build cyber capabilities

Local Government Association

Approach

Advice not assurance

Building capabilities

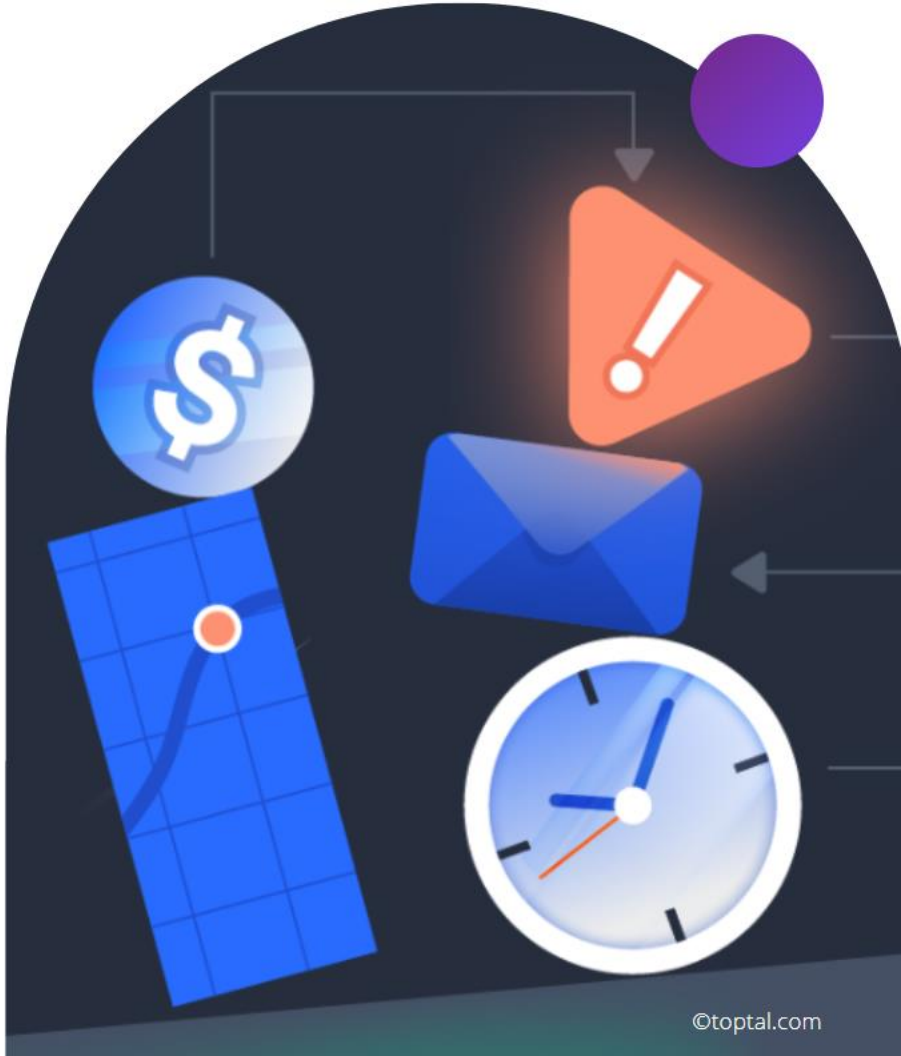
A focus on culture

Cyber 360 Framework

Common challenges for councils

Local Government Association

- It's IT's responsibility
- Poor risk management
- Unknown assets
- Minimum standards
- Supplier lifecycle
- Need for guidance
- Policies unknown
- Blind trust in backups
- Vulnerabilities not prioritised
- Alerts untuned
- No targeted training
- Plans untested



“... but everything is fine!”

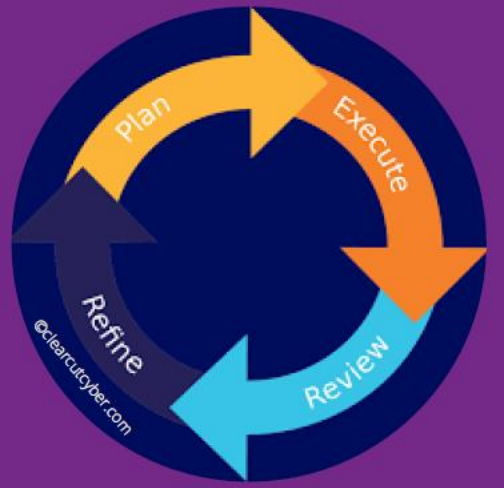
You don’t need to have a specific issue to benefit from any part of our offer. Councils have found the exercises useful for:

- Increasing awareness of cyber security
- Building knowledge and skills across service areas
- Framing cyber security challenges in the context of the whole organisation
- Providing a friendly external opinion

Local Government Association

Cyber Reaction Exercises

Cyber reaction exercises help councils to establish how well they might react to a cyber incident, and to practice their response in a safe, constructive environment.



01 **Incident Response**

02 **Business Continuity**

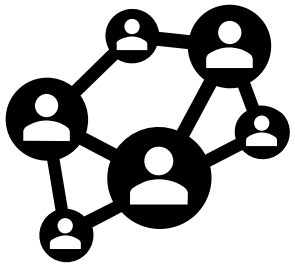
An Evolving Threat Landscape

Geopolitical insecurity

- Increase in cyber threats since the start of the Russia-Ukraine war

Greater cybercrime accessibility

- Technological advances are enabling more creative forms of attack and a greater number of threat actors

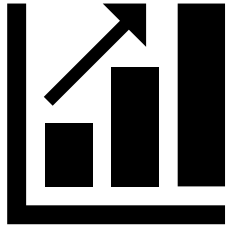


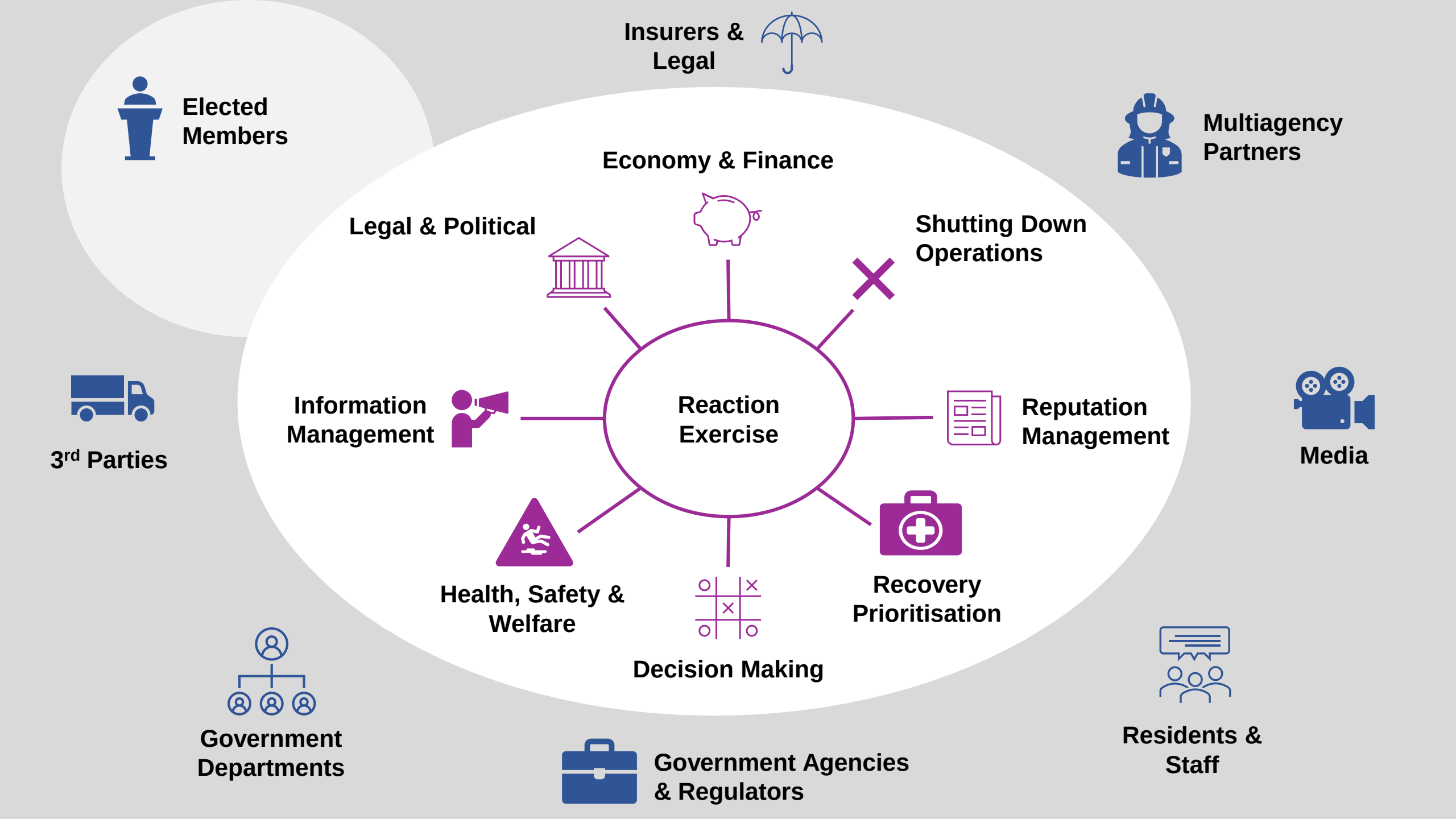
More complex ecosystems

- Organisations are concerned about the cyber resilience of supply chains

Unprecedented pace of change

- Organisations are struggling to adapt quickly enough to a dynamic threat landscape



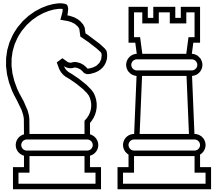

Insurers & Legal
Elected Members
Multiagency Partners
Economy & Finance
Legal & Political
Shutting Down Operations
Information Management
Reaction Exercise
Reputation Management
3rd Parties
Media
Health, Safety & Welfare
Recovery Prioritisation
Decision Making
Government Departments
Government Agencies & Regulators
Residents & Staff

What is a Business Continuity Reaction Exercise?

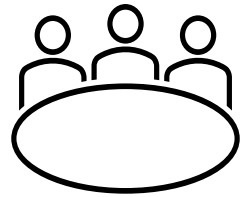
- A collaborative session to validate the organisations incident response and crisis management processes when responding to a simulated cyber incident.
- Discussions will help identify and prioritise opportunities for improvement in planning and management.
- This will ensure alignment at all levels, with consideration of key partners, third-parties, and other stakeholders.

Understand the impact of a cyber incident and response & recovery capabilities

Rehearse and embed key processes around BCP/DR and crisis management



Understand your roles and responsibilities and the function of senior management in the incident response process



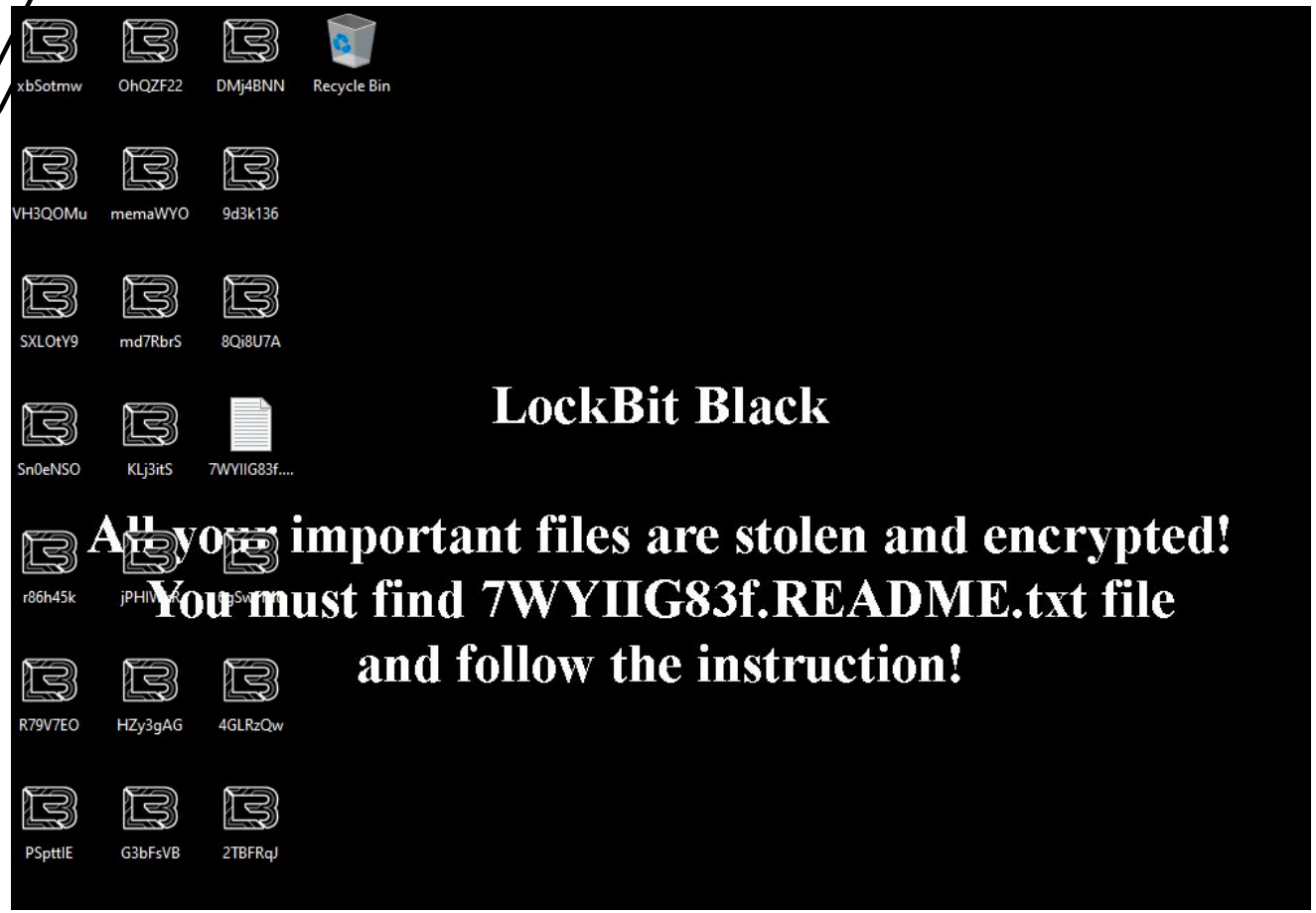
Further discuss and agree on potential 'grey areas' of an incident response and provide guidance on areas for improvement

Situation Report

Monday, 05:00

Example Inject

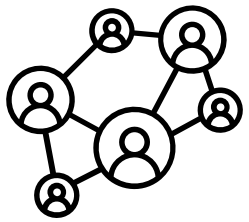
40 Minutes



- Critical systems are encrypted.
- Main network disconnected pending further security analysis.
- The root cause analysis will take several days to complete, maybe longer.
- Significant disruption expected across all services as the working week begins.
- Managed Security Service Provider has been activated and the National Cyber Security Centre has been notified.
- Potentially attacked by Lockbit, a financially motivated threat actor group.
- Primary communications platforms are unavailable.

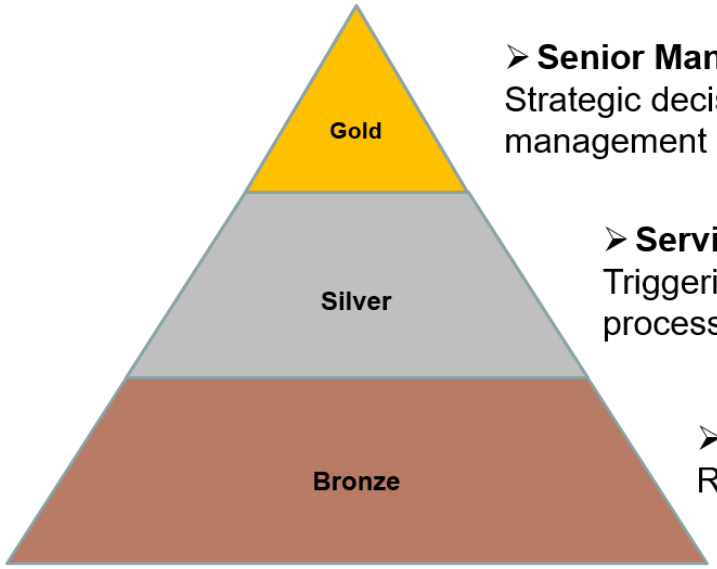
Reaction Exercise Overview

- Validate robustness and resilience of Incident Response Plans
- Practice roles and responsibilities and information flows to effectively rehearse an incident response



Exercise participants:

Exercises should be conducted at all levels for coherent response and organisational resilience



➢ **Senior Management/Leadership**
Strategic decision making and crisis management

➢ **Service Leads**
Triggering incident response processes

➢ **Operational Staff**
Response coordination

Indicative Workflow:

Kick-off & Discovery

Confirm objectives, scope, potential scenarios and key dates. Understand process for senior sign off. Scenario development.

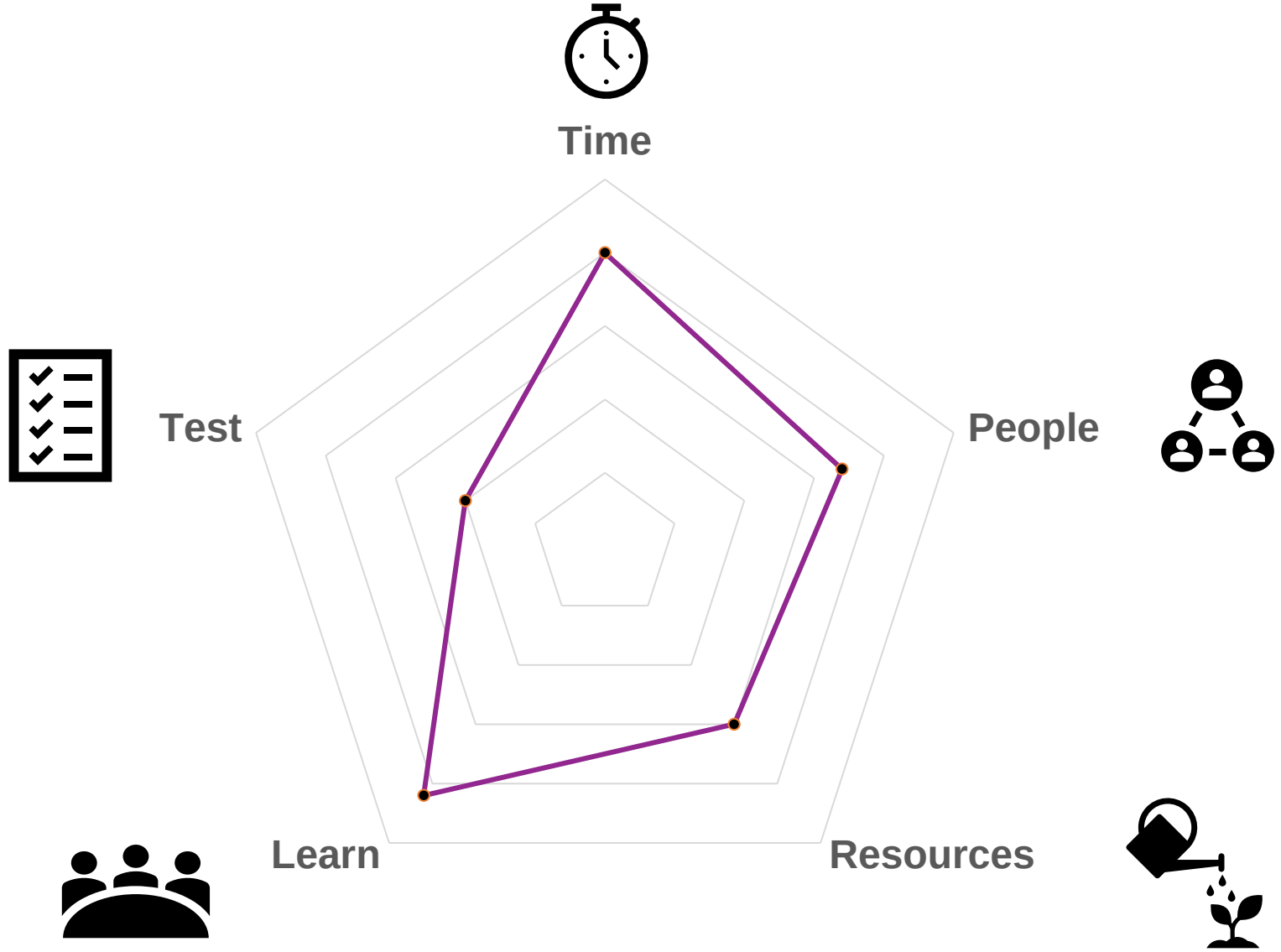
Exercise Delivery

Scenario finalisation. Facilitation of the exercise to promote discussion around response processes, whilst validating roles and responsibilities and documentation.

Post Exercise Reporting

Provision of a detailed report outlining strengths and recommendations for improvement, prioritised for further development by the organisation.

Scenario Development



Watch this space

LGA Supported Exercise

We will support you through the full process to deliver the first exercise

Exercise Guide

We will provide a reference guide to support future exercises

Scenario Bank

We will build a library of exercise scenarios, available on our website

Local Government Association

Meet the Bespoke Cyber Support Team

Jamie Cross
Programme Manager

Daniella Akinfenwa
Programme Support

Dave Sifleet
Senior Technical Specialist

Billy Ruston
Response Specialist

Richard Lewis
Technical Specialist

Local Government Association

Feedback

"We highly valued our Cyber 360, that considered a wide range of issues within the review scope. These extended beyond typical technical controls to the 'softer' but important issues of culture, leadership and governance. Gaining input from a range of organisations from across the sector added extra value."

Matt Prosser, Chief Executive, Dorset Council

Local Government Association

Feedback

"Since the Cyber 360 team spoke with the Council, there's been agreement to extend the cyber security training to Members."

Jason Tillyard, Head of ICT & Transformation, Dartford Borough Council

Local Government Association

Contact Us

020 7664 3000

lgacybersecurity@local.gov.uk

www.local.gov.uk

18 Smith Square, London, SWIP 3HZ