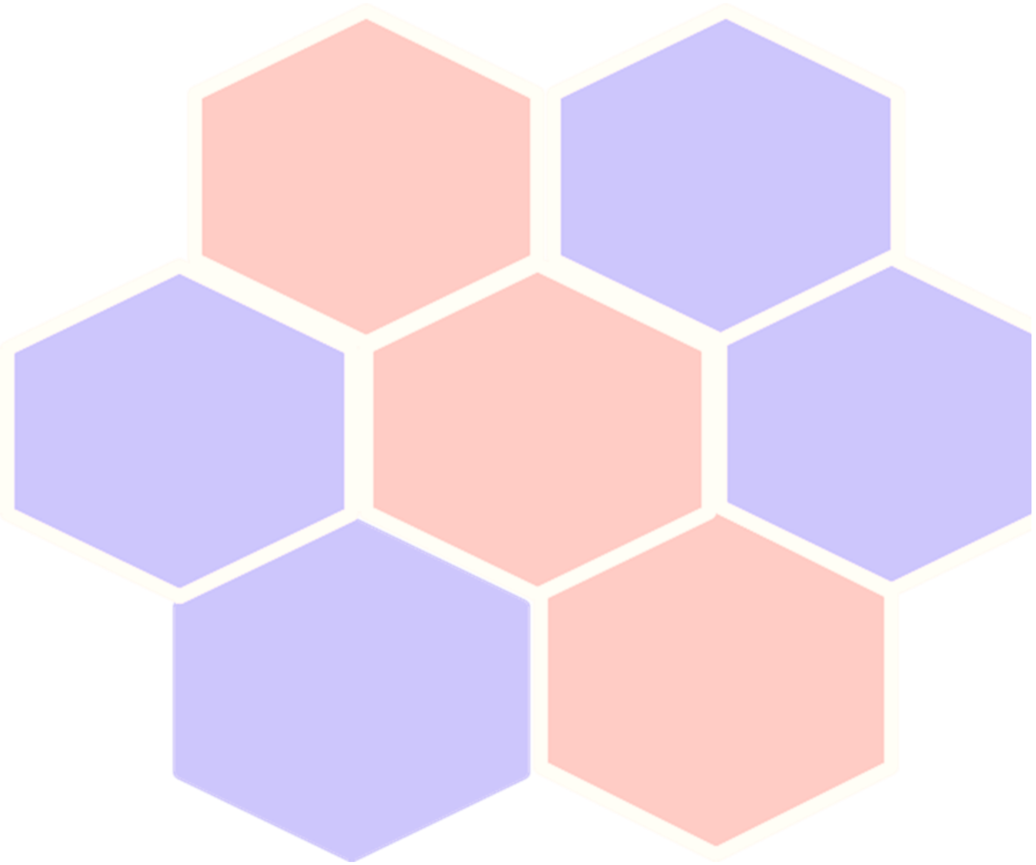
Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

Resilient by Design: Key strategic design principles for a civic cyber resilient organisation



CYBERUK STRATEGY

Think Cyber
Think Resilience

iStandUK
BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

The **Think Cyber Think Resilience** initiative is a National Cyber Security Programme (NCSP) funded collaboration between the Ministry for Housing, Communities and Local Government and IStandUK (the Local e-Government Standards Body) that brings strategic leaders, policy makers and practitioners together from across the local public and resilience sectors to work with NCSP partners to develop shared cyber resilience learning and mentoring resources to support wider awareness across civic sector organisations.

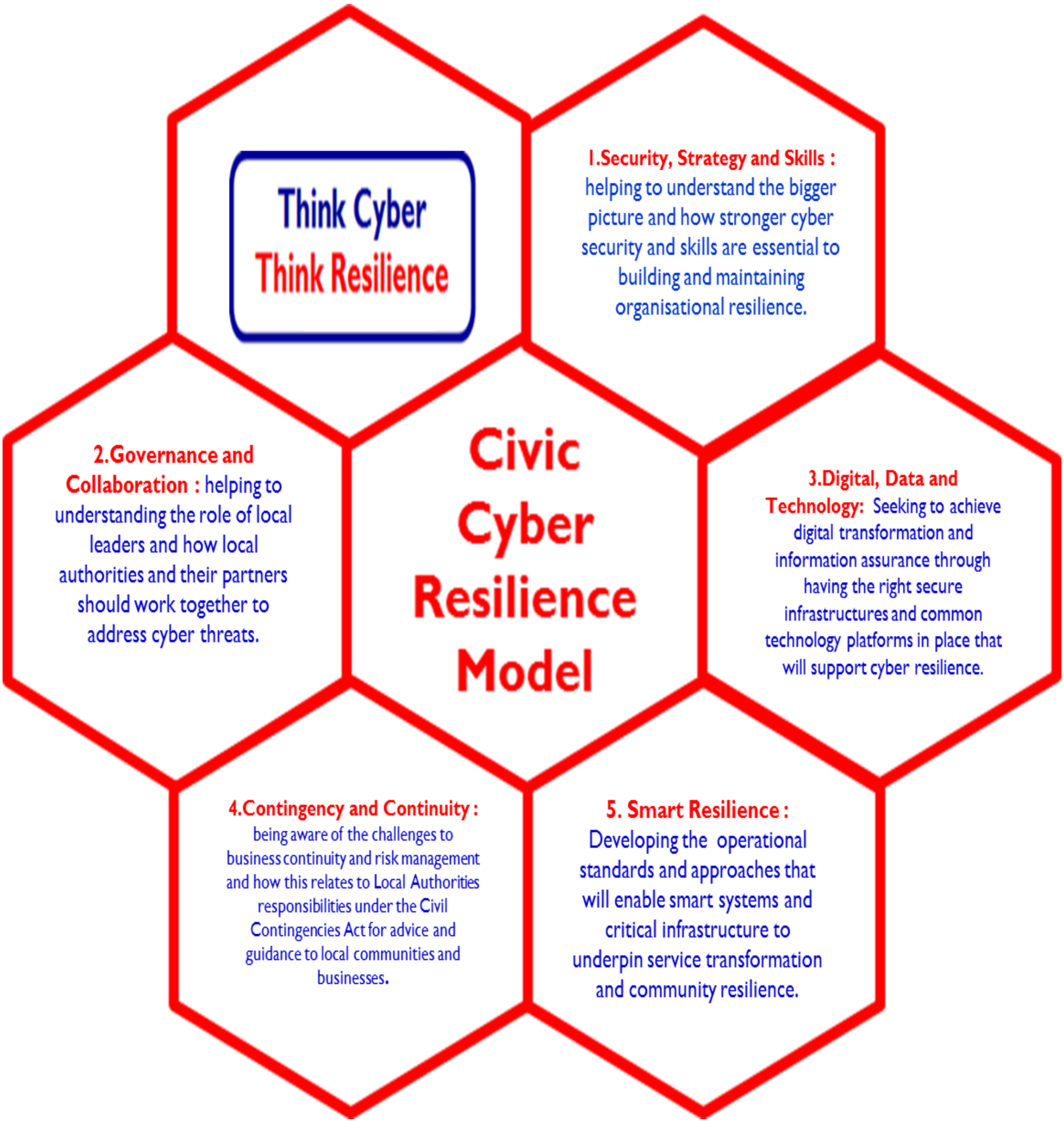
Since its launch in 2015 **Think Cyber Think Resilience** has run a wide scale programme of "*Building Resilience Together*" briefing seminars, conferences and exercises across English local authorities and local resilience forums to help induct over 2000 local public sector leaders and practitioners in the wider National Cyber Security Strategy. The initiative works closely with the National Cyber Security Centre, Cabinet Office Civil Contingencies Secretariat and the Local Government Association.

Think Cyber Think Resilience has hosted a series of Local Leadership in Cyber Society strategic round table events at **St George's House Windsor** to support wider thought leadership across government, local public service, private and academic sectors. **Think Cyber Think Resilience** was awarded international exemplar status by the **OECD Observatory of Public Sector Innovation** in April 2017 for its innovative approach to shared learning in support of civic cyber resilience.

Resilient by Design – Key strategic design principles for a civic cyber resilient organisation

This booklet outlines the design principles contained in the **Civic Cyber Resilience Model** (CCRM) developed by the **Think Cyber Think Resilience** initiative in conjunction with the wider National Cyber Security Programme and local public sector leaders, policymakers, practitioners and **St George's House Windsor**. The model (see Fig 1 below) covers five broad themes and is sub-divided by a set of key design principles.

Fig 1- Civil Cyber Resilience Model


Think Cyber
Think Resilience
1.Security, Strategy and Skills : helping to understand the bigger picture and how stronger cyber security and skills are essential to building and maintaining organisational resilience.
2.Governance and Collaboration : helping to understanding the role of local leaders and how local authorities and their partners should work together to address cyber threats.
Civic Cyber Resilience Model
3.Digital, Data and Technology: Seeking to achieve digital transformation and information assurance through having the right secure infrastructures and common technology platforms in place that will support cyber resilience.
4.Contingency and Continuity : being aware of the challenges to business continuity and risk management and how this relates to Local Authorities responsibilities under the Civil Contingencies Act for advice and guidance to local communities and businesses.
5. Smart Resilience : Developing the operational standards and approaches that will enable smart systems and critical infrastructure to underpin service transformation and community resilience.

CCRM sets out the strategic headlines and provides relevant prompts for the actions you need to consider in devising your own cyber resilience strategy. It will help you to identify, assess and mitigate the threats to your organisation.

- ❑ **Theme 1: Strategy, Security and Skills** - helping to understand the bigger picture and how stronger cyber security and skills are essential to building and maintaining organisational resilience:-

- ❑ **Strategy** - Understanding the issues and why digital and cyber resilience is central to operational effectiveness and efficiency.

    - ❑ Develop a strategic overview why digital and cyber resilience matters and the key security measures and skills required.
    - ❑ Understanding the local dimension and need for organisation wide awareness.
    - ❑ Strategically manage incidents and the organisational understanding of cyber threats.
    - ❑ Prioritise partnerships and collaboration to address cyber-crime and fraud issues

- ❑ **Security** – highlighting the key steps and controls to ensure that public bodies are cyber resilient.

    - ❑ Embed active cyber defence approaches built around enhanced internet security.
    - ❑ Adopt the key security steps, controls and processes.
    - ❑ Understand how to reduce the impact of attacks and establish strong incident reporting and response processes throughout your organisation.
    - ❑ Access and use security policy frameworks and standards in accordance with Government Security advice.

- ❑ **Skills** – gaining the essentials skills that people and organisations need to have in place to be cyber resilient.

    - ❑ Access National Cyber Security Centre (NCSC) resources and use the Cyber Essentials and skills guides.
    - ❑ Use NCSC approved training.
    - ❑ Support SIRO and Information Assurance Guidance training.
    - ❑ Provide access to skills training including Massive Open Online Courses/ online resources.

- ❑ **Theme 2 : Governance and Collaboration** - helping to understanding the role of local leaders and how local authorities and their partners should work together to address cyber threats:-

- ❑ **Leadership** – understanding what leaders need to know and how they need to place cyber awareness at the heart of organisational resilience.

    - ❑ Place the issue at the heart of corporate business and communications – not just an IT issue.
    - ❑ Understand the key role of SIRO and wider Governance implications.
    - ❑ Ensure Board level leadership accesses the right help and advice.
    - ❑ Know and use the key questions Leaders need to ask.

- ❑ **Collaboration** – recognising that cyber resilience is about building strong partnerships both within and across organisational boundaries.

    - ❑ Join and actively participate in the Cyber Security Information Sharing Partnership.
    - ❑ Work with WARPS and Local Resilience Forums.
    - ❑ Adopt boundary spanning approaches and learning across other sectors.
    - ❑ Develop and share "what works" Case Studies.

- ❑ **Cyber Culture** - embed a People Centred Culture around cyber resilience across the organisation.

    - ❑ Understanding how the key focuses of organisational leaders around cyber need to support and complement each other.
    - ❑ Be aware of the threats and opportunities and what to do about them.
    - ❑ Prioritise and decide what matters in terms of resources, systems and technologies.
    - ❑ Monitor and manage data so as to get the right Management Information and help to manage the corporate risks.

- ❑ **Theme 3 : Digital, Data and Technology** - Seeking to achieve digital transformation and information assurance through having the right secure infrastructures and common technology platforms in place that will support cyber resilience:-

- ❑ **Digital Transformation** – having the right foundations in place to build cyber secure digital services and grow a vibrant and expanded local digital and cyber resilient economy.

  - ❑ Ensuring that localities have the standards in place to adopt cyber resilience digital solutions and services. .
  - ❑ Ensuring that digital by default and cyber secure by default is at the heart of digital service delivery.
  - ❑ Ensuring that organisations support wider growth and innovation across the local cyber and digital sectors.
  - ❑ Support smart procurement by adopting Crown Commercial Service (CCS) Cyber procurement frameworks on Digital Market place.

- ❑ **Data and Information** – ensuring that cyber resilience is underpinned by strong and effective data handling, information assurance and information governance.

  - ❑ Have a robust Bulk Data and Information Assurance policy.
  - ❑ Ensure you have effective training for both leaders and staff.
  - ❑ Regularly access and use published Data Handing guidance.
  - ❑ Develop a culture of trust, both within and beyond your organisation.

- ❑ **Common Technology and Platforms** – seeking to adopt best of breed common technology solutions and approaches to underpin operational cyber resilience.

  - ❑ Adopt secure networks and robust connectivity through the use of assured products and technologies.
  - ❑ Look to adopt common technology components, and best practise models in step with the rest of Government.
  - ❑ Support local partnerships in the development and deployment of new platform components and deliver integrated Mission IT.
  - ❑ Adopt a security as an enabler ethos in the adoption and deployment of all systems.

- ❑ **Theme 4 : Contingency and Continuity** - being aware of the challenges to business continuity and risk management and how this relates to Local Authorities responsibilities under the Civil Contingencies Act for advice and guidance to local communities and businesses:-

- ❑ **Civil Contingencies** – understanding Local Authorities role under the Civil Contingencies Act to provide advice and guidance to local businesses and communities around cyber resilience.

    - ❑ Monitor Civil Contingencies Act compliance.
    - ❑ Work with the wider Civil Contingencies community both central and local.
    - ❑ Partner with Local Resilience Forums and use Resilience Direct.
    - ❑ Focus on supporting Communities and Business that may be impacted by cyber-attacks.

- ❑ **Business Continuity** – ensuring that internal Business Continuity Arrangements are focussed on identifying and combatting cyber vulnerabilities and challenges.

    - ❑ Use the Business Continuity Management Toolkit.
    - ❑ Promote wider local understanding of the issues by raising public and business awareness.
    - ❑ Undertake Cyber Security Planning and conduct regular cyber exercises.
    - ❑ Maintain Incident Response and supervisory control systems throughout your organisation.

- ❑ **Risk Management** – understanding the organisational risk appetite so as to help manage the risks and consequences of a cyber-attack and understand how organisations need to plan as to how to recover from a major incident.

    - ❑ Understand how risk assessment processes can help.
    - ❑ Learn how to define your organisation's risk appetite.
    - ❑ Identify the Cyber risk management issues for your locality.
    - ❑ Understand how to tackle Cyber Risks and reduce their impact.

❑ **Theme 5 : Smart Resilience** – Developing the operational standards and approaches that will enable smart systems and critical infrastructure to underpin service transformation and community resilience:-

❑ **Smart Systems** - developing the common operational standards and approaches to the smart critical infrastructure systems underpinning devolved cyber resilient organisations

- ❑ Work to embed cyber resiliency capabilities into Smart Critical Infrastructures across the locality.
- ❑ Look to leverage prior public sector investment in local smart digital/cyber solutions such as Internet of Things.
- ❑ Prioritise the development of smart approaches to combatting cyber-crime and fraud
- ❑ Adopt and develop common Smart City Standards

❑ **Service Transformation** – understanding how effective cyber security and resilience is essential to underpin service transformation and digital delivery.

- ❑ Keep in touch with the wider Public Service Transformation agenda.
- ❑ Understand the changing role of data sharing and strong data analytics.
- ❑ Adopt common service design standards based on User Centric Focused Delivery.
- ❑ Understand how digital platforms and approaches can support wider change.

❑ **Community Resilience** – recognising that good cyber resilience is an essential precondition for resilient communities and cities.

- ❑ Champion whole place approaches to building resilient communities and businesses that are based on common standards.
- ❑ Actively contribute to the creation of resilient Infrastructure and Communication systems.
- ❑ Understand how focussed leadership and innovation can help to create resilient communities.
- ❑ Foster collaborative working and networked learning around online safety and combatting cyber-crime.

Think Cyber Think Resilience: Resilient by Design

The design principles contained in this booklet are based on Civic Cyber Resilience Model developed by the **Think Cyber Think Resilience** initiative in conjunction with the wider National Cyber Security Programme, St George's House Windsor and local public sector leaders, policymakers and practitioners.

To learn more about how **Think Cyber Think Resilience** can help your organisation go to the accompanying online **Resilient by Design 2: Sources of online guidance on applying the Civic Cyber Resilience Model**, which contains extensive links to advice and guidance across all the themes outlined in this booklet visit http://istanduk.org/cyber-resilience/

In addition we would recommend that you accessing the following National Cyber Security Programme partners web pages as a way of keeping your organisation up to date with the latest wider cyber resilience guidance :-

- ❑ **National Cyber Security Centre** – national technical authority for cyber security see (https://www.ncsc.gov.uk/)
- ❑ **Cyber Essentials and Cyber Essentials Plus** - national schemes that offers a sound foundation of basic cyber hygiene measures (https://www.ncsc.gov.uk/scheme/cyber-essentials)
- ❑ **Cyber Aware** - national campaign to improve the online safety, behaviour and confidence (https://www.cyberaware.gov.uk/)
- ❑ **Local Government Association** – cyber security information pages for local authorities (www.local.gov.uk)
- ❑ **St George's House** – for the Local Leadership in a Cyber Society Report (http://www.stgeorgeshouse.org/wp-content/uploads/2016/04/Local-Leadership-in-Cyber-Society-Report.pdf)
- ❑ **OECD Public Sector Innovation Observatory –** for the **Think Cyber Think Resilience** international exemplar case study**.** (https://www.oecd-opsi.org/)

Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

The **Think Cyber Think Resilience** initiative is a National Cyber Security Programme (NCSP) funded collaboration between Ministry for Housing, Communities and Local Government and IStandUK (Local e-government standards body) that brings strategic leaders, policy makers and practitioners together from across the local public service and resilience sectors to work with NCSP partners to develop shared cyber resilience learning and mentoring resources to support wider awareness across civic sector organisations.

To find out more see http://istanduk.org/cyber-resilience/ or contact:
cyber-resilience@communities.gsi.gov.uk

Think Cyber Think Resilience: Awarded OECD Public Sector Innovation Exemplar Status April 2017

Published by INetwork in support of the National Cyber Security Programme 2016/2021