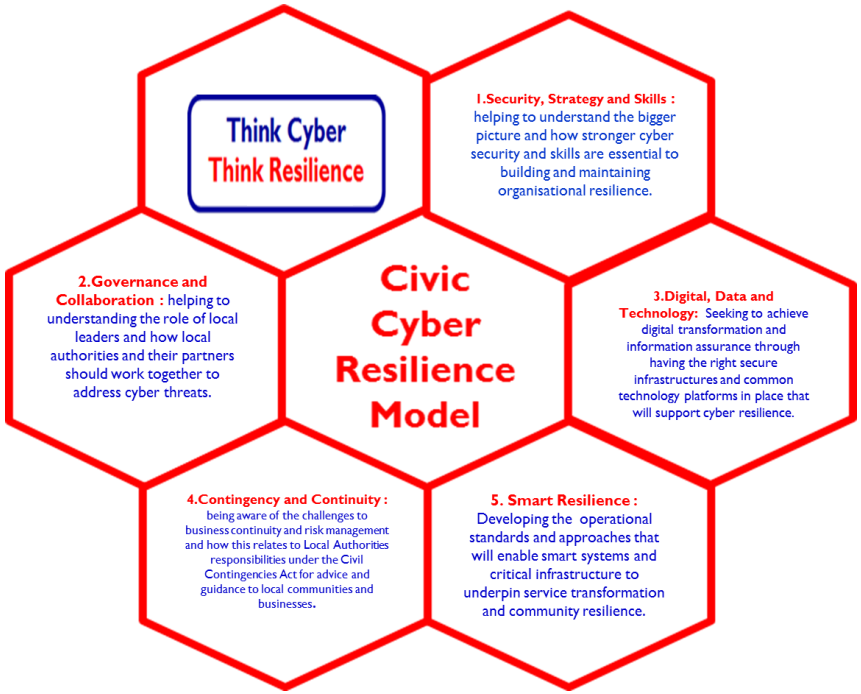
Think Cyber
Think Resilience

Resilient by Design 2: Sources of online guidance on applying the Civic Cyber Resilience Model

Building Resilience Together :
Briefing Paper



CYBERUK STRATEGY

Think Cyber
Think Resilience

iStandUK
BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

Think Cyber Think Resilience

Resilient by Design 2: Sources of online guidance on applying the Civic Cyber Resilience Model

Building Resilience Together : Briefing Paper

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.

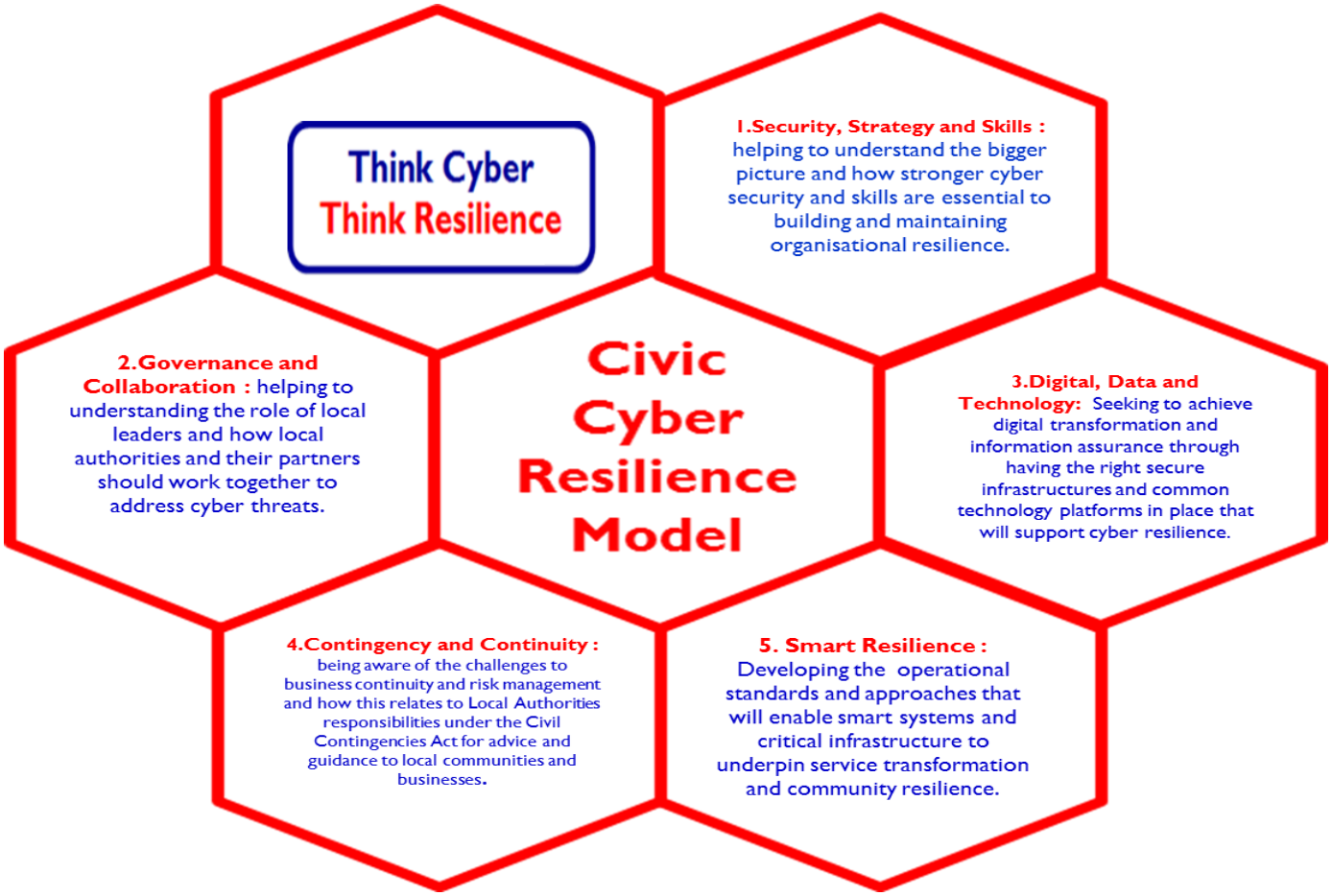
Think Cyber Think Resilience has hosted a series of Local Leadership in Cyber Society strategic round table events at **St George's House Windsor** to support wider thought leadership across government, local public service, private and academic sectors. **Think Cyber Think Resilience** was awarded international 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.

ST GEORGE'S HOUSE

OECD Observatory of Public Sector Innovation

Resilient by Design 2: Sources of online guidance on applying the Civic Cyber Resilience Model

This booklet provides links to guidance and background reading to the design principles contained in the **Civic Cyber Resilience Model** 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 following five broad themes and is sub-divided by a set of key design principles. **Fig 1- Civil Cyber Resilience Model**



❑ **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:-

1.1.0	**1.1 STRATEGY - Understanding the issues and why digital and cyber resilience is central to operational effectiveness and efficiency.**		
		Key NCSC and Gov.UK Guidance	**Further Reading**
1.1.1	**Develop a strategic overview why digital and cyber resilience matters and the key security measures and skills required.**	**The National Cyber Security Strategy 2016-21 (NCSS) was published in November 2016. It sets out the Government's key strategic objectives in defence of the economy and privacy of citizens from the increasing threat of cyber-attacks. The full strategy can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf** **One of the key deliverables of the NCSS is the creation of the National Cyber Security Centre (NCSC). Part of GCHQ but designed to "*protect our critical services from cyber-attacks, managing major incidents and improve the underlying security of the UK Internet*". You can find more information about the NCSC on its website at: https://www.ncsc.gov.uk/** **NCSC also publishes blog posts on Cyber Strategy at: https://www.ncsc.gov.uk/topics/cyber-strategy**	**The NCSS follows on and complements the wider National Security Strategy see: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015** **For related Government Cyber Policy publications see: https://www.gov.uk/government/policies/cyber-security** **For related strategy updates from the NCSC see: https://www.ncsc.gov.uk/topics/government-strategy**
1.1.2	**Understanding the local dimension and need for organisation wide awareness.**	**In March 2015, DCLG published *Understanding Local Cyber Resilience* a guide for local government see: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf** **This guidance outlined the key cyber threats facing local government along with some actions that can be taken to reduce the risks or impacts from cyber threats.**	**DCLG, with iNetwork and other partners, run a series of OECD award winning cyber resilience awareness raising events. Learning from those events, along with other supporting material can be found at: http://istanduk.org/cyber-resilience/**

1.1.3	Strategically manage incidents and the organisational understanding of cyber threats.	One of the main functions of the NCSC is Incident Management see: https://www.ncsc.gov.uk/incident-management NCSC also manages the Cyber-security Information Sharing Partnership (CiSP) and all Public Sector Organisations are encouraged to join CiSP at: https://www.ncsc.gov.uk/cisp	NCSC guidance on reporting a cyber incident can be found at: https://www.ncsc.gov.uk/articles/get-help-significant-cyber-incident-guidance
1.1.4	Prioritise partnerships and collaboration to address cyber-crime and fraud issues.	An established principle of cyber resilience is that everyone is responsible for cyber security; within the organisation and across the supply chain. This requires effective partnerships and collaboration – raising awareness about cyber threats through corporate leadership, communications, education and training: https://www.ncsc.gov.uk/news/awareness-only-first-step	Cyber-crime and computer enabled fraud is a growing area of concern – whatever your business if you hold financial data or personal information about people, you could be target. Action Fraud is the UK's national fraud and cyber-crime reporting centre – see: http://www.actionfraud.police.uk/ The National Crime Agency (NCA) has more information about cyber-crime at: http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime For more information about actions being taken by the NCA to tackle cyber crime. See: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

1.2.0	1.2 SECURITY – highlighting the key steps and controls to ensure that public bodies are cyber resilient.		
		Key NCSC and Gov.UK Guidance	Further Reading
1.2.1	Embed active cyber defence approaches built around enhanced internet security.	NCSC is responsible for updated cyber security guidance see: https://www.ncsc.gov.uk/index/guidance For information about 20 Critical Controls* to improve an organisations cyber defences see: https://www.ncsc.gov.uk/guidance/20-critical-controls	20 Critical Controls was originally published by the Centre for the Protection of Critical Infrastructure (CPNI). Most of the functions of CPNI have now transferred to NCSC. You can find out more about CPNI at: https://www.cpni.gov.uk/about-cpni For an update on CPNI and Cyber Security see: https://www.cpni.gov.uk/cyber-security Information about the Public service Network (PSN) can

			be found at: https://www.gov.uk/government/groups/public-services-network
1.2.2	Adopt the key security steps, controls and processes.	For information on how organisations can protect themselves in cyberspace see 10 Steps to Cyber Security: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security	For advice and guidance covering the day to day management of an organisation's Operational Security see: https://www.ncsc.gov.uk/topics/operational-security For advice on protecting the Physical Security of the places where people work, and the locations of systems, services and networks see: https://www.ncsc.gov.uk/topics/physical-security NCSC has not yet published advice on protecting the Personal Security of an organisations people but appears to be planning to do so at: https://www.ncsc.gov.uk/topics/personnel-security
1.2.3	Understand how to reduce the impact of attacks and establish strong incident reporting and response processes through.	The latest NCSC advice on explaining how basic security controls can protect organisations from the most common cyber attacks is at: https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact	NCSC also manages the Cyber-security Information Sharing Partnership (CiSP) and all Public Sector Organisations are encouraged to join CiSP at: https://www.ncsc.gov.uk/cisp If you require third-party assistance in dealing with a cyber-security incident, you can find information on NCSC certified Cyber Incident Response companies at: https://www.ncsc.gov.uk/scheme/cyber-incidents
1.2.4	Access and use security policy frameworks and standards in accordance with Government Security advice.	All organisations should consider having Security Policy Frameworks defining access controls and standards. Documents relating to the UK Government security policy frameworks can be found at: https://www.gov.uk/government/collections/government-security#security-policy-framework	The Government security policy framework provides central internal protective security policy and risk management for all government departments, associated bodies and partners handling government information. It is the source on which all localised security policies should be based see: https://www.gov.uk/government/publications/security-policy-framework

1.3.0	1.3 SKILLS – gaining the essentials skills that people and organisations need to have in place to be cyber resilient.		
		Key NCSC and Gov.UK Guidance	Further Reading
1.3.1	Access National Cyber Security Centre (NCSC) resources and use the Cyber Essentials and skills guides.	There is an acknowledged shortage of people with the right cyber skills and it will take time to fill this skills gap. Therefore, it is important that the public sector shares and makes use of good practice guidance. The NCSC is tasked with helping to fill this skills gap and to promote guidance on cyber issues see: https://www.ncsc.gov.uk/	Cyber Essentials is a government-backed and industry-supported scheme to guide organisations in protecting themselves against cyber threats see: https://www.cyberessentials.ncsc.gov.uk/
1.3.2	Use NCSC approved training.	NCSC guidance on Skills & Training can be found at: https://www.ncsc.gov.uk/topics/skills-and-training .	GCHQ has certified Master's degrees in cyber security and closely related fields see: https://www.ncsc.gov.uk/information/gchq-certified-degrees The NCSC guide '10 Steps To Cyber Security' concerns User Education and Awareness see: https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness Government has also provided advice to businesses on cyber skills see: https://www.gov.uk/government/publications/cyber-security-skills-a-guide-for-business

1.3.3	Support SIRO and Information Assurance Guidance training.	Information Assurance (see: CIAN 2015 02 Information Assurance Maturity Model (IAMM) Interim Guidance.pdf) can help an organisation protect itself from cyber-attacks. Local authorities may already have appointed Information Assurance Officer(s) and Senor Information Risk Owner(s).	For advice on Digital Information Security see: https://www.gov.uk/service-manual/technology/securing-your-information For archived information about the SIRO role see: http://webarchive.nationalarchives.gov.uk/+/http://www.nationalarchives.gov.uk/documents/information-management/the-role-of-the-siro.pdf
1.3.4	Provide access to Massive Open Online Courses/ online resources.	A massive open online course (MOOC) is an online course aimed at unlimited participation and open access via the web. In 2014 the then Coalition Government supported development of a MOOC on cyber security see: https://www.gov.uk/government/news/government-supports-uks-next-generation-of-cyber-security-professionals	More information about the cyber security MOOC including how to join the next presentation of the course see: https://www.futurelearn.com/courses/introduction-to-cyber-security

❑

❑ **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:-

2.1.0	**2.1 LEADERSHIP – understanding what leaders need to know and how they need to place cyber awareness at the heart of organisational resilience.**		
		Key NCSC and Gov.UK Guidance	**Further Reading**
2.1.1	**Place the issue at the heart of corporate business and communications – not just an IT issue.**	**Government guidance for non-executive directors, which covers corporate issues such as balancing risk and reward can be found at: https://www.gov.uk/government/publications/cyber-security-balancing-risk-and-reward-with-confidence**	**See also guidance on partnerships, collaboration and raising awareness at: https://www.ncsc.gov.uk/news/awareness-only-first-step**
2.1.2	**Understand the key role of SIRO and wider Governance implications.**	**CPNI produced its 'Passport to Good Security' aimed at Senior Executives it has 20 key actions for senior managers and boards need to ask: https://www.cpni.gov.uk/advice/Passport-to-Good-Security/**	**While local authorities may not have a designated SIRO role, somewhere within their organisation the duties of the SIRO should be part of good governance and security. National Archives used to provide guidance on the SRIO and an archived version of that guidance can be at: http://webarchive.nationalarchives.gov.uk/+/http://www.nationalarchives.gov.uk/documents/information-management/the-role-of-the-siro.pdf**
2.1.3	**Ensure Board level leadership accesses the right help and advice.**	**"Everyone with senior executive or Board level responsibility needs to have concise strategic information to guide their decision-making, risk management and governance activities" – see introduction to CPNI Passport: https://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport** **[Note sure why following link, which deals with cyber security skills, is in this section: https://www.gov.uk/government/publications/cyber-security-skills-a-guide-for-business]**	**See also CPNI advice on cyber security for business at: https://www.cpni.gov.uk/cyber-security** **[This link http://www.cpni.gov.uk/highlights/cyber-advice-businesses/ redirects to above]**

2.1.4	Know and use the key questions Leaders need to ask.	10-steps to cyber security is a key piece of guidance from the NCSC; it includes key questions that CEO/Boards need to know how to answer: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility	Embedding Security Behaviour Change contains advice from CPNI on getting the right security behaviour culture in organisations see: https://www.cpni.gov.uk/embedding-security-behaviour-change CPNI also provides wider advice on Personnel & People Security at: https://www.cpni.gov.uk/personnel-and-people-security

2.2.0	2.2 COLLABORATION – recognising that cyber resilience is about building strong partnerships both within and across organisational boundaries.		
		Key NCSC and Gov.UK Guidance	Further Reading
2.2.1	Join and actively participate in the Cyber Security Information Sharing Partnership.	Managed by the NCSC, the Cyber Information Sharing Partnership (CiSP) is joint Industry & Government initiative providing a forum for cyber security discussion from beginner through to expert level. Public sector organisations are encouraged to join CiSP; local authorities can join the Local Government node in CiSP and (where established) the relevant cross sector regional node. https://www.ncsc.gov.uk/cisp	CERT-UK (now part of NCSC) provided the following generic guidance on CiSP for the DCLG/iNetwork cyber awareness events: http://istanduk.org/wp-content/uploads/2016/05/08-cisp-application-steps.pdf
2.2.2	Work with WARPS and Local Resilience Forums.	A WARP (Warning, Advice and Reporting Point) is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions: https://www.ncsc.gov.uk/articles/what-warp Local Resilience Forums (LRF) bring together key organisations that work together in response to duties under the Civil Contingencies Act (CCA): https://www.gov.uk/government/publications/the-role-of-local-resilience-forums-a-reference-document	For information about National Local Authority WARP see: http://www.nlawarp.net/ - More information about LRF and how to contact your nearest LRF see: https://www.gov.uk/guidance/local-resilience-forums-contact-details Please Note: CCA does not cover cyber related incidents but some LRF are exploring their potential role in handling the impacts of a cyber-attack.

!2.2.3	Adopt boundary spanning approaches and learning across other sectors.	Every organisation and everybody is potential target for those responsible for cyber attacks, the public sector can therefore learn from others. Active involvement in CiSP, your local WARP and nearest LRF helps to share. As will active involvement with local businesses, communal organisations, etc. Local Authorities may wish to consider what role they can play, under Community Safety, in promoting good cyber practice: http://www.local.gov.uk/topics/community-safety	Understanding Security & Privacy (https://www.gov.uk/service-manual/service-standard/understand-security-and-privacy-issues) is included in the UK Government Digital Service Standards (https://www.gov.uk/service-manual/service-standard) Advice on Vulnerability and Penetration testing is available at: https://www.gov.uk/service-manual/technology/vulnerability-and-penetration-testing Guidance from the Bank of England on it's CBEST Vulnerability Testing Framework is at: https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity
2.2.4	Develop and share "what works" Case Studies.	As well as learning from other sectors, Local Government should share and learn from within the sector see, for example, the Gloucestershire Safer Cyber Forum (GSCF) https://www.safercybergloucestershire.uk/	Resilience Direct provides a browser based tool to enable efficient and secure (accredited to Official level) exchange of information during both routine planning and response to emergencies. Consider joining Civic Cyber Resilience working group on Resilience Direct (membership sign-on required): https://www.ordnancesurvey.co.uk/business-and-government/case-studies/resilience-direct.html

2.3.0	2.3 CYBER CULTURE - embed a People Centred Culture around cyber resilience across the organisation.		
		Key NCSC and Gov.UK Guidance	Further Reading
2.3.1	Understanding how the key focuses of organisational leaders around cyber need to support and complement each other.	Cyber affects everyone decisions taken across an organisation – Finance, HR, Communications, IT – could have adverse impacts on your cyber defences: https://www.ncsc.gov.uk/guidance/10-steps-executive-summary	Board level guidance for CEO & Board Members: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility

2.3.2	Be aware of the threats and opportunities and what to do about them.	The NCSC publishes regular updates on threats and guidance, is anyone in your organisation reading them? https://www.ncsc.gov.uk/threats#ataglance	See also the DCLG guidance for local government at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf
2.3.3	Prioritise and decide what matters in terms of resources, systems and technologies.	Every organisation is unique and there are one-size-fits-all strategies for cyber so it is for each organisation to determine priorities, resources, etc. The NCSC offers advisory guidance to help make you make informed decisions at: https://www.ncsc.gov.uk/guidance	See also: 10 Steps Executive Summary: https://www.ncsc.gov.uk/guidance/10-steps-executive-summary 10 Steps Board Level Responsibilities: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility Common Cyber Attacks: Reducing the Impacts: https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact NCSC Infographics can help bring cyber to life and they free to re-use at: https://www.ncsc.gov.uk/articles/infographics-cesg
2.3.4	Monitor and manage data so as to get the right Management Information and help to manage the corporate risks.	Cyber Essentials is for all organisations, of all sizes, and in all sectors - we encourage all to adopt the requirements as appropriate to their business. https://www.cyberessentials.ncsc.gov.uk/	More information about monitoring can be found the 10 Steps guidance at: https://www.ncsc.gov.uk/guidance/10-steps-monitoring

- **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:-

3.1.0	**3.1 DIGITAL TRANSFORMATION – having the right foundations in place to build cyber secure digital services and growth a vibrant and expand local digital and cyber resilient economy.**		
		Key NCSC and Gov.UK Guidance	**Further Reading**
3.1.1	**Ensuring that localities have the standards in place to adopt cyber resilience digital solutions and services. .**	**GDS leads the drive by Government Departments to develop digital services. NCSC provides independent guidance on digital services at: https://www.ncsc.gov.uk/topics/digital-services**	**For more about the Digital by Default Service Standards see: https://www.gov.uk/service-manual/service-standard** **Information about the Local Government Digital Service Standard is at: https://localgov.digital/service-standard**
3.1.2	**Ensuring that digital by default and cyber secure by default is at the heart of digital service delivery.**	**NCSC guidance on security and digital services can be found at: https://www.ncsc.gov.uk/guidance/digital-service-security**	**NCSC guidance on designing secure digital services can be found at: https://www.ncsc.gov.uk/guidance/digital-services-building-secure-digital-service**
3.1.3	**Ensuring that organisations support wider growth and innovation across the local cyber and digital sectors.**	**Digital services and cyber security are acknowledged as of growing importance to economic growth, which is as a key role for local government see: https://www.ncsc.gov.uk/guidance/digital-services-designing-secure-digital-service**	**LGA reports on transforming local public services using technology and digital tools: http://www.local.gov.uk/sites/default/files/documents/transforming-public-servi-2a5.pdf**

3.1.4	Support digital smart procurement by adopting the official Crown Commercial Service (CCS) Cyber procurement frameworks on Digital Market place.	Crown commercial Services (CCS) helps Government and the wider public sector to buy common goods or services – for more information see: https://www.gov.uk/government/organisations/crown-commercial-service CCS provides framework agreements that you can use to procure goods and services. You can search for existing agreements (including those covering cyber related services) at: http://ccs-agreements.cabinetoffice.gov.uk/ NCSC provides guidance on becoming a certified cyber security consultancy at: https://www.ncsc.gov.uk/articles/become-certified-cyber-security-consultancy	Digital Marketplace aims to make it clearer, simpler and faster for the public sector to buy digital products or services. For more information about Digital Marketplace see the GDS digital market place blog at: https://digitalmarketplace.blog.gov.uk/ To search for people, products or services on the Digital Marketplace go to: https://www.digitalmarketplace.service.gov.uk/

3.2.0	3.2 DATA & INFORMATION – ensuring that cyber resilience is underpinned by strong and effective data handling, information assurance and information governance.		
		Key NCSC and Gov.UK Guidance	Further Reading
3.2.1	Have a robust Bulk Data and Information Assurance policy.	Local Government, like many other organisation, rely on the information they hold about their service users but 'personal data' has value to cyber attackers – see NCSC guidance on protecting personal data at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main	Protecting personal data is linked to Information Assurance and this archived guidance explains the Information Assurance Maturity Model: https://www.ncsc.gov.uk/guidance/information-assurance-maturity-model-and-assessment-framework-gpg-40 The Information Commissioner's Office also provides information on data protection and on the new General Data Protection Regulation (GDPR): https://ico.org.uk/ https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

3.2.2	Ensure you have effective training for both leaders and staff.	The National Archives provides training in Information Assurance and Cyber Security aimed at different roles from Board Level to Information Asset Owners- see: http://www.nationalarchives.gov.uk/information-management/training/	There is also specific guidance from NCSC in handling data in transit: https://www.ncsc.gov.uk/topics/data-transit
Nage ment 3.2.3	Regularly access and use published Data Handing guidance.	Information Commissioner's Office publishes guidance for organisations at: https://ico.org.uk/for-organisations/	Published in February 2017, the 4th edition of the Local Public Services Data Handling Guidelines provides revised and updated guidance: see link at https://www.nlawarp.net/
3.2.4	Develop a culture of trust, both within and beyond your organisation.	CESG provided guidance on Information Assurance at Enterprise Level, although a few years old, it is now on the NCSC website: https://www.ncsc.gov.uk/content/files/guidance_files/GPG%2028%20-Improving%20IA%20at%20the%20Enterprise%20Level%20-%20issue%201.3%20-%20Oct%2015%20-%20NCSC%20Web.pdf	Similar cyber security & information assurance guidance can be found under Digital and Technology skills at: https://www.gov.uk/government/collections/digital-data-and-technology-job-roles-in-government

3.3.0	3.3. COMMON TECHNOLOGY & PLATFORMS – seeking to adopt best of breed common technology solutions and approaches to underpin operational cyber resilience.		
		Key NCSC and Gov.UK Guidance	Further Reading
3.3.1	Adopt secure networks and robust connectivity through the use of assured products and technologies.	For those using the Public Services Network (PSN) go to: https://www.gov.uk/government/groups/public-services-network	More information about the future of PSN can be found at: https://governmenttechnology.blog.gov.uk/2017/03/16/a-secure-future-for-psn-assurance/

3.3.2	Look to adopt common technology components, and best practise models in step with the rest of Government.	Common Technology Services (CTS) uses shared components and standards to provide flexible, efficient and cheaper Cloud based solutions: https://governmenttechnology.blog.gov.uk/2016/06/03/a-new-approach-to-common-technology-services/ The GDS blog on CTS can be found at: https://governmenttechnology.blog.gov.uk/category/common-technology-services/	See also the Government Transformation Strategy: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 -
3.3.3	Support local partnerships in the development and deployment of new platform components and deliver integrated Mission IT.	Cyber security requires collaboration between teams within an organisation and across the organisations supply lines; within the public sector (especially local government) there is also scope for local partnership working:	LocalGov Digital is a network for digital practitioners in local government with an aim to raise standards in web provision and the use of digital by councils across the country, and to create a digital framework that is flexible enough to respond to local needs : https://localgov.digital The Local Digital Coalition maintains resources created by the DCLG Local Digital Programme to enable organisations involved in local public service transformation to collaborate on digital transformation initiatives https://www.localdigitalcoalition.uk/
3.3.4	Adopt a security as an enabler ethos in the adoption and deployment of all systems.	Security as an enabler recognises the benefits to the business or organisation of including the security of their services, systems, processes & people in the design, development & build processes – rather than as an add-on later: https://www.gov.uk/service-manual/technology#protecting-user-information	The newly established NCSC is looking into taking proactive action to defend the UK from cyber attacks, they call this Active Cyber Defence: https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

- **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:-

4.1.0	**4.1 CIVIL CONTINGENCIES – understanding Local Authorities role under the Civil Contingencies Act to provide advice and guidance to local businesses and communities around cyber resilience.**		
		Key NCSC and Gov.UK Guidance	**Further Reading**
4.1.1	**Monitor Civil Contingencies Act compliance.**	**The Civil Contingencies Act 2004 provides a single framework for Civil Protection in the UK including local arrangements for civil protection (part 1) and emergency powers (part 2): http://www.legislation.gov.uk/ukpga/2004/36/contents**	**See also: https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others**
4.1.2	**Work with the wider Civil Contingencies community both central and local.**	**Local Resilience Forums have been established under the Civil Contingencies Act to bring together organisations involved in Civil Protection: https://www.gov.uk/government/publications/the-role-of-local-resilience-forums-a-reference-document**	**Note: Cyber Security (security against a cyber-attack) and Cyber Resilience (resistance to & ability to recover from a cyber-attack) are not covered by the Civil Contingencies Act. However, cyber is beginning to feature on the Risk Register of some Local Resilience Forums. Engaging with Local Resilience Forums will help with collaboration and building partnerships etc.**
4.1.3	**Partner with Local Resilience Forums and use Resilience Direct.**	**Information about all the Local Resilience Forums and contact details can be found at: https://www.gov.uk/guidance/local-resilience-forums-contact-details Resilience Direct is an online network enabling civil protection practitioners to work together – across geographical and organisational boundaries – during the preparation, response and recovery phases of an event or emergency: https://www.gov.uk/guidance/resilient-communications**	**Guidance on – Resilience in society: infrastructure, communities and businesses can be found at: https://www.gov.uk/guidance/resilience-in-society-infrastructure-communities-and-businesses**

4.1.4	Focus on supporting Communities and Business that may be impacted by cyber-attacks.	There is guidance on planning, preparing and exercising for Civil Protection at: https://www.gov.uk/guidance/emergency-planning-and-preparedness-exercises-and-training	Note: CERT-UK used to run table-top cyber exercises but this appears to have stopped now that they have become part of NCSC. However, NCSC does offer various certifications schemes for suppliers – including systems and penetration testing – see: https://www.ncsc.gov.uk/marketplace

4.2.0	4.2 **BUSINESS CONTINUITY** – ensuring that internal Business Continuity Arrangements are focussed on identifying and combatting cyber vulnerabilities and challenges.		
		Key NCSC and Gov.UK Guidance	Further Reading
4.2.1	Use the Business Continuity Management Toolkit.	For many organisations one of the most immediate consequences of a cyber attack is the disruption of its business. Business Continuity Management (BCM) offers techniques for identifying critical services, resources, etc; protection of these critical elements; and planning for their recovery (where necessary). Organisations need to think about how they include cyber related issues in their BCM: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/137994/Business_Continuity_Managment_Toolkit.pdf	One example of a Local Authority including cyber in their resilience planning is the City of London: Business resilience planning considerations – see: https://www.cityoflondon.gov.uk/business/support-promotion-and-advice/business-continuity/Documents/business-resilience-planning-considerations.pdf
4.2.2	Promote wider local understanding of the issues by raising public and business awareness.	Government advice on Business Continuity Planning can be found at: https://www.gov.uk/government/publications/business-continuity-planning	Expecting The Unexpected: Business continuity in an uncertain world: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/376381/Expecting_the_Unexpected_Reviewed.pdf
4.2.3	Undertake Cyber Security Planning and conduct regular cyber exercises.	City of London: Business resilience planning considerations: https://www.cityoflondon.gov.uk/business/support-promotion-and-advice/business-continuity/Documents/business-resilience-planning-considerations.pdf	NCSC offer various certifications schemes for suppliers – including systems, penetration testing – see: https://www.ncsc.gov.uk/marketplace

4.2.4	Maintain Incident Response and supervisory control systems throughout your organisation.	See NCSC Incident management team advice on how they identify and respond to cyber security incidents, assist with their mitigation, and build our understanding of cyber security threats. In the event of significant cyber security incidents, they provide direct technical support and cross-government co-ordination of response activities: https://www.ncsc.gov.uk/incident-management and https://www.ncsc.gov.uk/articles/get-help-significant-cyber-incident-guidance	Also link-up with the CiSP (Cyber-security Information Sharing Partnership) -Managed by the NCSC, CiSP provides a forum for cyber security discussion from beginner through to expert level. It's also a platform where organisations can share intelligence gathered from their own computer networks.

4.3.0	4.3 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.		
		Key NCSC and Gov.UK Guidance	Further Reading
4.3.1	Understand how risk assessment processes can help.	Risk management is about managing the impact of uncertainty; every activity entails some degree of uncertainty: Risks arise when uncertainties have the potential to impact on activities: https://www.ncsc.gov.uk/guidance/risk-management-introduction	The risks which digital technologies, devices and media bring are manifest. Cyber risks are not only issues for the IT team, an organisation's risk management function needs to understanding the constantly evolving risks as well as the practical tools and techniques available to address them: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
4.3.2	Learn how to define your organisation's risk appetite.	Every organisation will have to determine for themselves which risks they need to protect (and which consequences can be ignored). Government guidance on national risks can be found at: https://www.gov.uk/guidance/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed	Institute of Risk Management guidance on cyber risks: https://www.theirm.org/media/2293893/IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

4.3.3	Identify the Cyber risk management issues for your locality.	Wider guidance, from the NCSC, on technology and information risk management can be found at: https://www.ncsc.gov.uk/guidance/risk-management-collection	Part of the NCSC guidance, are these principles of risk management: https://www.ncsc.gov.uk/guidance/risk-management-principles
4.3.4	Understand how to tackle Cyber Risks and reduce their impact.	NCSC advice and guidance on governing, communicating and making decisions about risk: https://www.ncsc.gov.uk/topics/risk-management	NCSC summary of risk methods and frameworks: https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks

- **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:-

5.1.0	**5.1 SMART SYSTEMS - developing the common standards and approaches to the smart critical infrastructure systems underpinning devolved cyber resilient organisations**		
		Key NCSC and Gov.UK Guidance	**Further Reading**
5.1.1	**Work to embed cyber resiliency capabilities into Smart Critical Infrastructures across the locality.**	**SmartRes - Smart Resilience Indicators for Smart Critical Infrastructures: http://www.smartresilience.eu-vri.eu/**	**See also GM-Connect: https://www.greatermanchester-ca.gov.uk/news/article/39/pioneering_data_service_to_connect_greater_manchester_to_improved_services**
5.1.2	**Look to leverage prior public sector investment in local smart digital/cyber solutions such as Internet of Things.**	**For information about previous programmes and current investment see the Public Service Transformation Academy at: http://publicservicetransformation.org/**	**For more about the Internet of Things (IoT) see: https://www.gov.uk/government/news/manchester-wins-10m-prize-to-become-world-leader-in-smart-city-technology**
5.1.3	**Prioritise the development of smart approaches to combatting cyber-crime and fraud**	**The Economic Crime Academy, run by City of London Police, provides information about cyber crime and related training: http://academy.cityoflondon.police.uk/economic_crime_academy_prospectus**	**For an example of police and academia partnership working on tackling online crime see: http://www.leedsbeckett.ac.uk/news/0416-west-yorkshire-police-and-leeds-beckett-university-unite/**

5.1.4	Adopt and develop common Smart City Standards	The Smart Cities Concept Model is a framework for improved interoperability and data sharing across the many types of organisation that serve local communities: http://istanduk.org/projects/smart-cities-concept-model/	

5.2.0	5.2 SERVICE TRANSFORMATION – understanding how effective cyber security and resilience is essential to underpin service transformation and digital delivery.		
		Key NCSC and Gov.UK Guidance	Further Reading
5.2.1	Keep in touch with the wider Public Service Transformation agenda.	The Local Digital Coalition maintains resources created by the DCLG Local Digital Programme to enable organisations involved in local public service transformation to collaborate on digital transformation initiatives https://www.localdigitalcoalition.uk/	
5.2.2	Understand the changing role of data sharing and strong analytics.	Data analytics and the newly role of Data Science is having a big impact on the way that data is used to improve or transform public services; find out more and keep up to date with developments at: https://dataingovernment.blog.gov.uk/category/data-science/	
5.2.3	Adopt common service design standards based on User Centric Focused Delivery.	See the NCSC Security Design Principles for Digital Services at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main	
5.2 4	Understand how digital platforms and approaches can support wider change.	Platforms will play an ever increasing role in the service transformation; for more information see the Government Transformation Strategy: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020	The Local Digital Coalition maintains resources created by the DCLG Local Digital Programme to enable organisations involved in local public service transformation to collaborate on digital transformation initiatives https://www.localdigitalcoalition.uk/

5.3.0	5.3 COMMUNITY RESILIENCE – recognising that good cyber resilience an essential precondition for resilient communities and cities.		
		Key NCSC and Gov.UK Guidance	Further Reading
5.3.1	Champion whole place approaches to building resilient communities and businesses that are based on common standards.	Local Government has a critical role to play in community resilience (including community cyber resilience) see How to make cities more resilient: a handbook for Local Government Leaders: http://www.unisdr.org/files/26462_handbookfinalonlineversion.pdf	
5.3.2	Actively contribute to the creation of resilient Infrastructure and Communication systems.	Resilient communications infrastructure goes beyond the boundary of an organisation and is an important building block for community resilience, for more about resilient communications see: https://www.gov.uk/guidance/resilient-communications	
5.3.3	Understand how focussed leadership and innovation can help to create resilient communities.	The 100 Resilient Cities initiative is helping cities around the world become more resilient to physical, social, and economic shocks and stresses, for more information see: https://www.rockefellerfoundation.org/our-work/initiatives/100-resilient-cities/	
5.3.4	Foster collaborative working and networked learning around online safety and combatting cyber-crime.	Cyber Aware is a cross-government awareness and behaviour change campaign aimed at small businesses and individuals, so that they adopt simple secure online behaviours to help protect themselves from cyber criminals: https://www.cyberaware.gov.uk/	Action Fraud is the UK's national reporting centre for fraud and cyber crime where you should report fraud if you have been scammed, defrauded or experienced cyber crime: https://www.actionfraud.police.uk/

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