Cyber resilience procurement requirements for smart London – Discovery Report for LOTI

12/02/2020

Sponsored by

London office of Technology and Innovation

SKILLS FORMATION
Enabling Transformation of Your Skills

Presenter – Meha Shukla
Director, Skills-Formation Ltd.
56 Acacia Avenue, Ruislip, HA48RG, UK
Email: uctzshu@ucl.ac.uk

Topics

1. Executive Summary

EXECUTIVE SUMMARY

Purpose: To investigate how we support local authorities to reduce as well as manage operational risks and liabilities of cyber-resilience issues during procurement life-cycle.

Objectives

- Translate high level available guidance into practical steps that boroughs can take to procure smart city services that are cyber-resilient.
- Produce control actions for boroughs to procure smart services mapped to LOTI's existing framework for Innovation in Procurement in a scalable manner.

Key Recommendation Areas:

1	2	3	4	5
Operating Model	Risk Management	Supplier Assessment	Research and Training	Supplier Development

Suggested Next steps

- Add detailed cyber-resilience measures to LOTI framework for consistency across boroughs
- Update based on NCSC and CPNI guidelines to be published, incorporate in national frameworks
- Coordinate prioritised work packages, coordinate with smart city teams across UK

6 Key Findings:

- Lack of a repeatable continuous method to procure secure and resilient smart services
- Resilience risks and liability exposure are not quantified consistently
- Lack of centralised procurement strategy and governance for smart city initiatives
- Lack of consistent method across boroughs to assess supply-chain resilience measures proportionate to risks for services
- Frameworks and standards are not necessarily relevant to local Governments
- Performance measures against resilience and security are not defined and monitored

2. Introduction

Delivering Resilience in London

"The value of resilience should be reflected in all levels of city governance, from citizen engagement and empowerment which helps build local resilient communities, through core city-level policy action on wellbeing, sustainability and good growth, to embedding, resilience thinking into policymaking which tackles long term challenges.

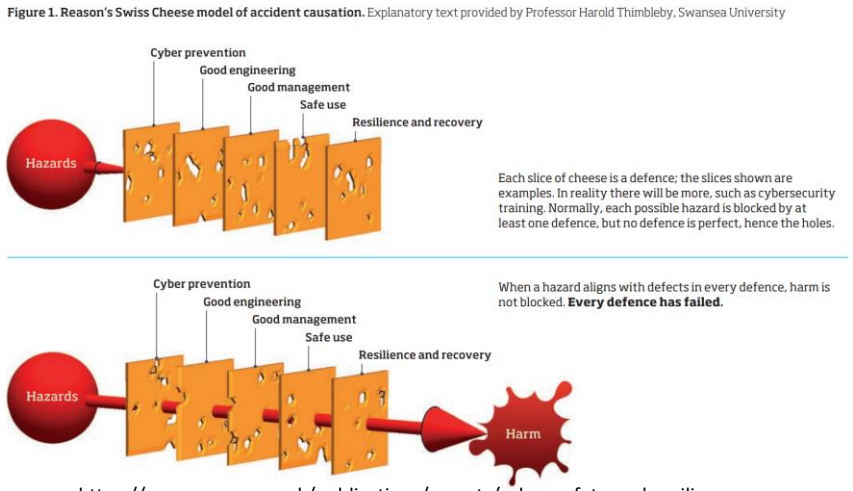
Resilience for **People**	**Building resilience for London's Communities**
Resilience for **Place**	**Developing resilience for London's physical environment and infrastructure**
Resilience for **Process**	**Designing resilience into governance**

https://www.london.gov.uk/sites/default/files/london_city_resilience_strategy_2020_digital.pdf

What do we mean by Resilience ?

"Resilience describes the capacity of a system to handle disruptions to operation. Cyber resilience refers to the ability of digital systems to **prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events**."

Cyber safety and resilience, Royal Academy of Engineering 2018



https://www.raeng.org.uk/publications/reports/cyber-safety-and-resilience

Examples:

- Service continuity or crisis management in event of cyber attack or a disruption event
- Disaster recovery alternatives – e.g. Covid 19
- Supplier providing services going bust
- Lack of governance for resilient processes
- People in key roles being unavailable

Reason's Swiss Cheese model of accident causation. Explanatory text provided by Professor Harold Thimbleby, Swansea University

Cyber security versus cyber resilience

Cyber Security by Design

- ✓ Establish context prior to designing a system
- ✓ Make compromises difficult
- ✓ Make disruption difficult
- ✓ Make compromise detection easier
- ✓ Reduce impact of a compromise

Cyber Resilience by Design

- ✓ Focus on critical processes and assets
- ✓ Support agility and architect for adaptability
- ✓ Reduce attack surfaces
- ✓ Assume compromised resources
- ✓ Expect adversaries to adapt

What are the key drivers for this project?

1 To help the borough officers implement their ideas consistently across London

(LOTI presentation Prototype1 :Plan-London Framework and Guidance – 04/05/2020) https://loti.london/projects/iotweek/

Sophie

Borough Officer

"We have so many ideas but we don't know how to implement them!

PROFILE

Jane has been working in Camden Borough for the last 8 years. She is usually involved in the procurement process for many projects, but is the first time she works with emerging technologies.

GOAL

Find the right solution for my borough.

FRUSTRATION

Lack of internal support and knowledge.

MOTIVATIONS

https://drive.google.com/file/d/1pwkaqqjnB36iX7sS345fj1lemQuqzfo-/view

2 Alignment required to Resilience Strategy for Smart London published by the Mayor

https://www.london.gov.uk/sites/default/files/london_city_resilience_strategy_2020_digital.pdf

3 Protect councils from signing up to risks and liabilities implicitly during procurement

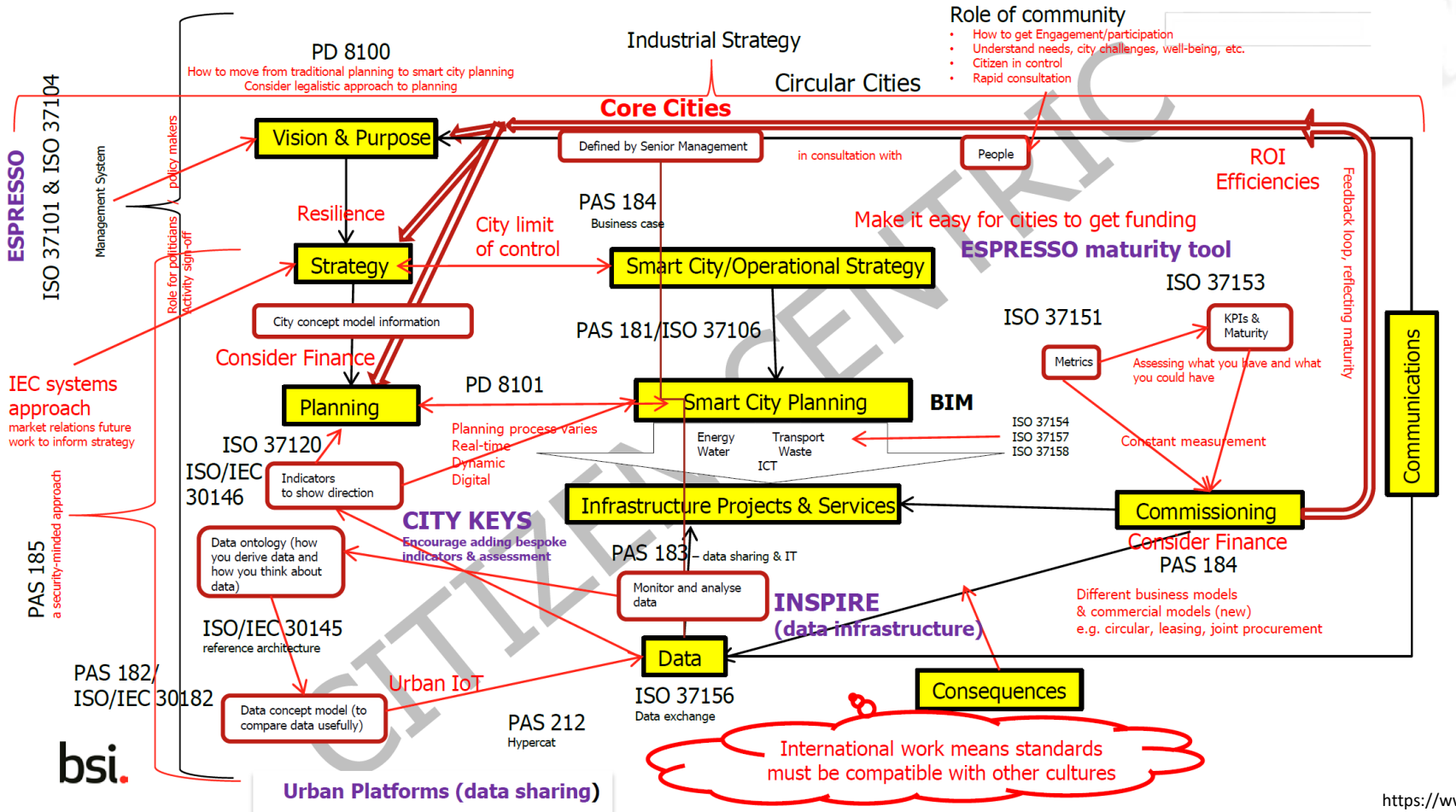
Framework/ Approach	Network ownership	Maintenance ownership	Risk Liabilities
Charge place Scotland	'Host' – local authority or organisation	Transport Scotland, on an ad hoc basis	With Transport Scotland and local authorities
Most current	Local authority	Local authority (monthly service fee paid to contractor)	With the central & local government
Private sector match			private sector
Central Southern			ween parties
Greater Manchester			rity
GULCS London Concession	Borough	Contracted supplier	Transferred to supplier
Oxford City Council	Local Authority	Contracted supplier	Transferred to supplier
Go Ultra Low Nottingham Concession	NCC owns underground network	Supplier	Transferred to supplier
Low-upfront cost models	Supplier	Supplier	Transferred to supplier

ACCOUNTABILITY OF RISKS AND LIABILITIES CANNOT BE TRANSFERRED

https://loti.london/projects/iotweek/

https://drive.google.com/file/d/1NJSYqBa0XF-0yJCjeDtrev39-ta4D4l0/view

Key challenge - Navigating through standards

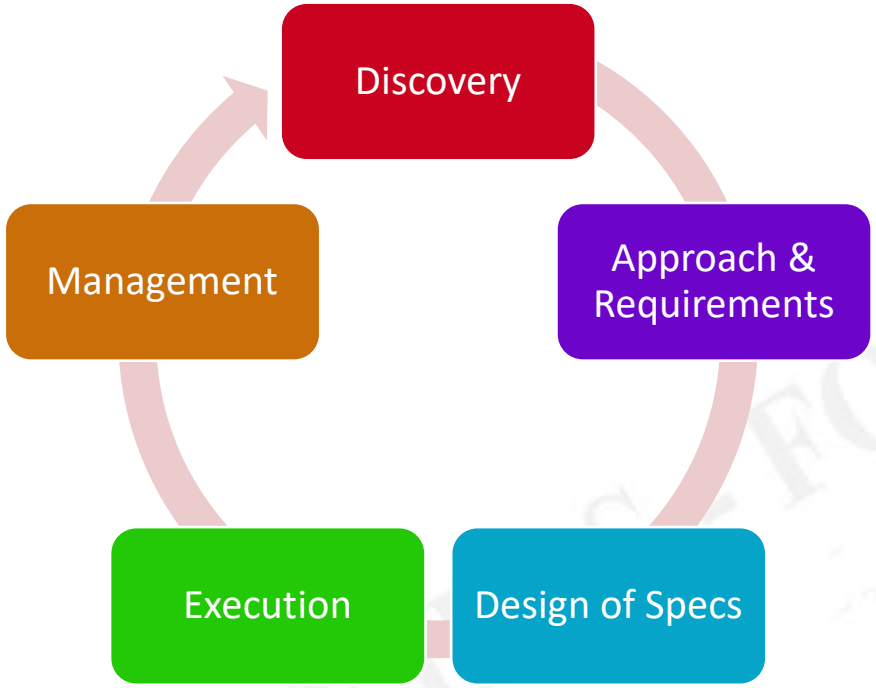


There's a well known saying about a tourist who asks one of the locals for directions. The local replies:

"Well sir, if I were you, I wouldn't start from here"

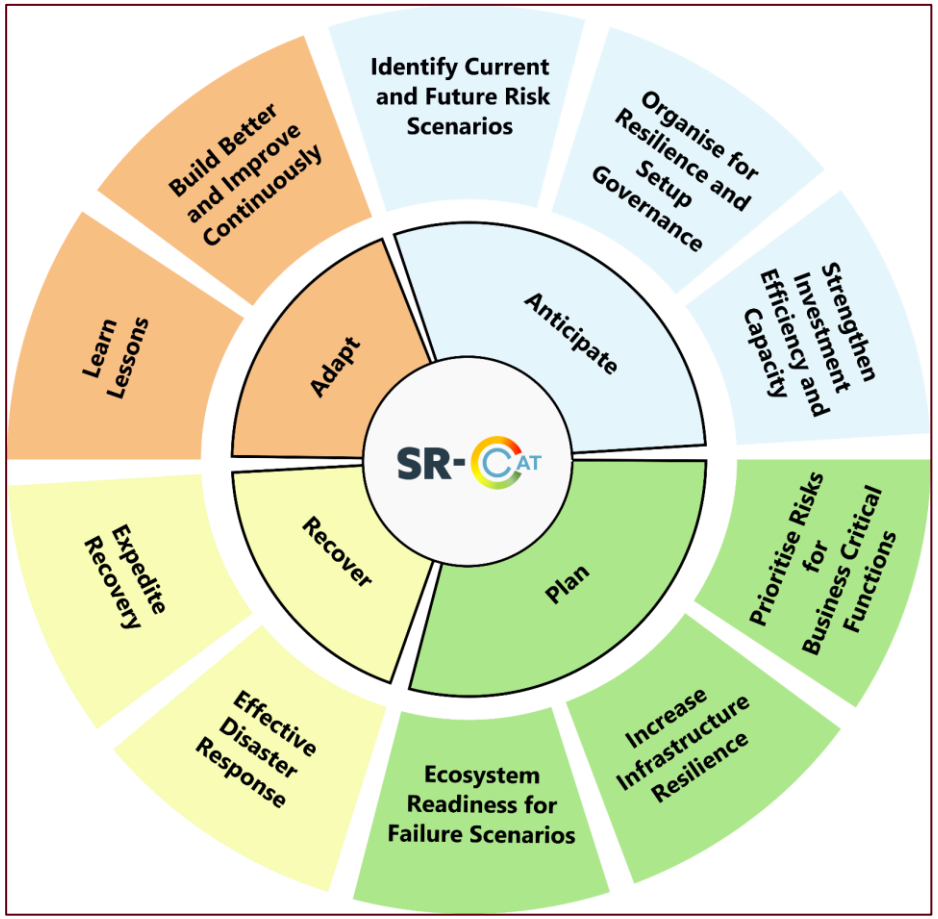
https://www.ubdc.ac.uk/media/1497/tom-digby-rogers-19-may-glasgow.pdf

LOTI Procurement Framework – Apply Resilience Lens



https://www.notion.so/84ea8097ae604bbb9cab8e29e84762d8?v=82e6cbfaa3a94c1c9d554d9628c9a2a2&p=7a1cb2b7428647a9ac1bff1c72241249
https://loti.london/resources/innovation-in-procurement-toolkit/

Resilience Framework used
Service Resilience Capability Assessment Tool (SR-CAT)



- Embeds risk-based service assurance standards by BSI based on NCSC guidelines and principles
- Classifies services based on the operational risks
- Provides proportionate 10 steps to cyber resilience assessment for each risk category within the procurement life-cycle
- Maps operational and liability risks to cyber resilience requirements
- Provides guidance to assess cyber resilience requirements using industry standard controls
- Provides guidance and trainings for adoption

3. Discovery work

Our Tasks

	Week1 22 Jan – 28 Jan 2021	Week2 29 Jan – 4 Feb 2021	Week3 5 Feb – 12 Feb 2021
Tasks	➢ Discussed risks of smart service procurements at London's local authorities ➢ Studied vendor assessment and assurance questionnaires	➢ Identified problems in procuring resilient smart services ➢ Arrived at key actionable controls	➢ Collated priorities across boroughs and worked out recommendations
Milestones	Initial workshops	Validation of problems and actions	Show and Tell

Our collaborative approach

9 London boroughs

6 workshops

4 Directorates

5 Consultations

25 Contributors

18 Standards applied

We conducted workshops with:
- South London partnership,
- Westminster and Kensington & Chelsea
- Brent & Greenwich

We spoke to:
- Directors (Business and IT)
- Architects
- Procurement officers
- Borough officers

We consulted with:
- NCSC and CPNI*
- MHCLG and DCMS
- Crown procurement services.

- We conducted regular progress reviews with LOTI
- We conducted desk research internally across international standards

Best Quote from the project:

"We spent all this time creating the questions and the one thing we clearly stated as needed, the vendor ignored"

Note: The outputs will also inform Meha Shukla's PhD research at UCL (permission will be sought prior to inclusion, *- ongoing)

4. Key Findings

Current Efforts

- LOTI is working closely with boroughs to define a consistent smart city procurements ecosystem
- LOTI is promoting inter region working with local and central Government initiatives
- NCSC and CPNI are working closely with LOTI and the boroughs to support them and ensure the national guidelines for cyber resilience are fit for purpose when released
- Procurement framework for cyber resilience risk management are being recognized as a must have and the ecosystem are keen to adopt when available
- Boroughs are engaging suppliers early in the procurement life-cycles to mitigate risks
- Boroughs are focused on user benefits and recognize resilience as an important element of any given service
- Boroughs are keen to adopt standards, guidelines and best practices

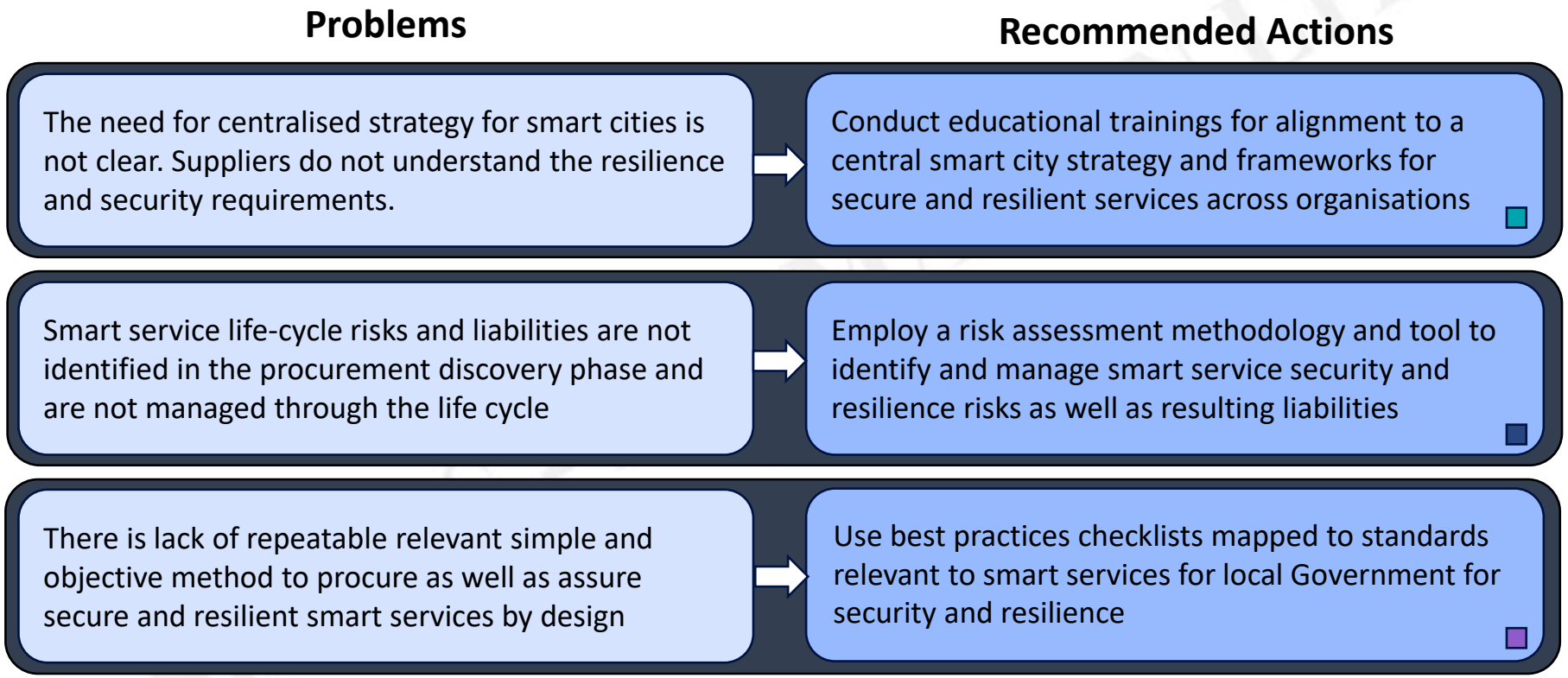
6 Key Findings that emerged from workshops

- **Resilience and Security**: There is a lack of guidance to create a repeatable continuous method to procure secure and resilient across location, people, cyber and other areas for smart services
- **Risk Management:** Resilience risks and liability exposure are not quantified in the procurement discovery phase through to contract management & dissemination consistently across boroughs.
- **Strategy and Governance:** There is no centralized procurement strategy and governance (spanning Business, IT, operations and services) across smart city initiatives and the need is also not widely understood. For example, shadow IT leads to operational and IT risks.
- **Supply change assurance:** There is a lack of consistent method to assess supply-chain resilience measures proportionate to risks for end-to-end services in all contract stages. The work-in-progress assessment questionnaires can be inconsistent, subjective, have limited coverage, complex to navigate, get incomplete responses from the suppliers and are not assessed for risks.
- **Frameworks and standards:** Frameworks and Standards for smart service security & resilience are not relevant to local Governments. They are not applied consistently.
- **Service Operations:** Performance measures against resilience and security are not defined and monitored consistently in contracts resulting in operational risks and lack of adaptation to the changing landscape.

Our 5 key principles to address these findings

- Consider cyber attacks and service disruptions business-as-usual
- Don’t reinvent the wheel, just realign it
- Resilient organizations to operate resilient services
- Break it down, articulate simple and easy to implement changes iteratively
- Collaborative working practices to support the journey to resilient smart services

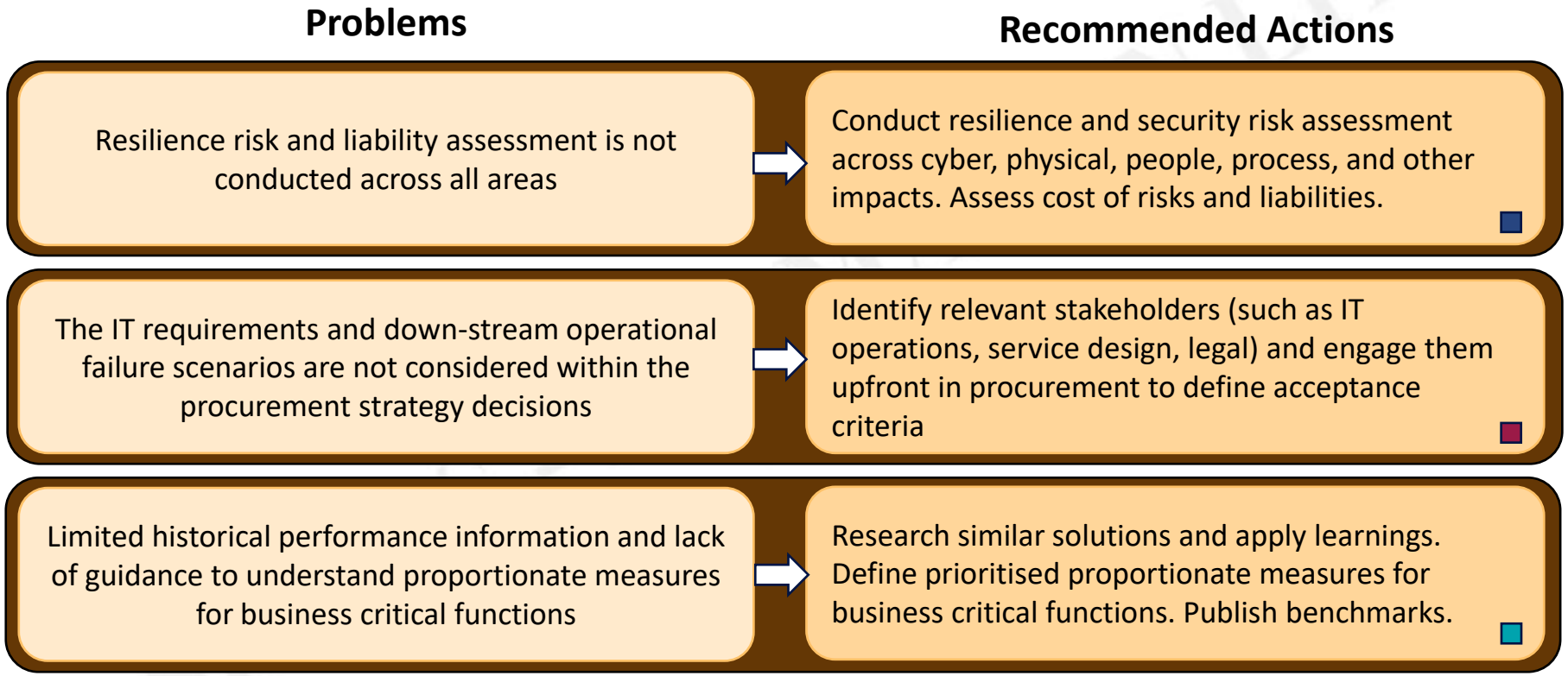
LOTI Procurement Step 1: Preparation



Selected Sources (for the more complete set of references please see appendix):

- NCSC Secure Design Principles
- NCSC Cyber Assessment Framework
- Crown Commercial Service Technology Products 2
- IoTSF IoT Security Compliance Framework

LOTI Procurement Step 2: Strategy



Selected Sources (for the more complete set of references please see appendix):

- NCSC Secure Design Principles
- NCSC Cyber Assessment Framework
- Crown Commercial Service Technology Products 2
- IoTSF IoT Security Compliance Framework

LOTI Procurement Step 3: Design

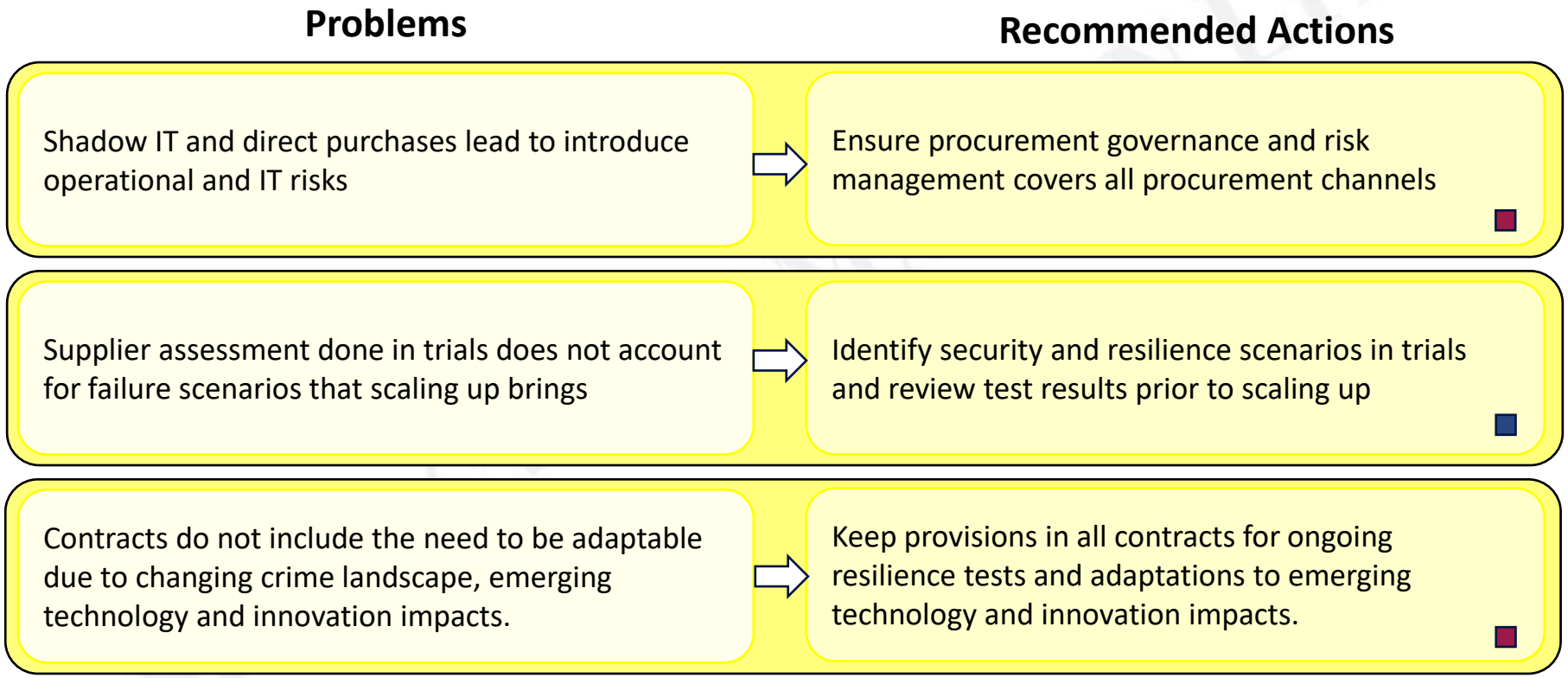
Problems	Recommended Actions
The specifications currently focus on data and cyber security, but misses connected impacts, service resilience and SLA*	Adapt shared checklist of resilience and security by design to assess impacts of connected services based on end-to-end SLA requirements
The supply-chain assessment questionnaire is laborious, is subjective, is not understood well by suppliers and is inconsistent across boroughs	Employ a tool based on guidelines, multiple choice questions and clear pass/fail selection for a set of holistic questions for consistent supplier assessment
The risks to service resilience and liabilities based on supplier assessment gaps are not understood. Insurance assumptions may not be valid	Use a method to analyse impact of supplier assessment gaps to resilience risks and liability. Validate feasibility of controls such as insurance.

Selected Sources (for the more complete set of references please see appendix):

- NCSC Secure Design Principles
- NCSC Cyber Assessment Framework
- Crown Commercial Service Technology Products 2
- IoTSF IoT Security Compliance Framework

SLA* - Service Level Agreement

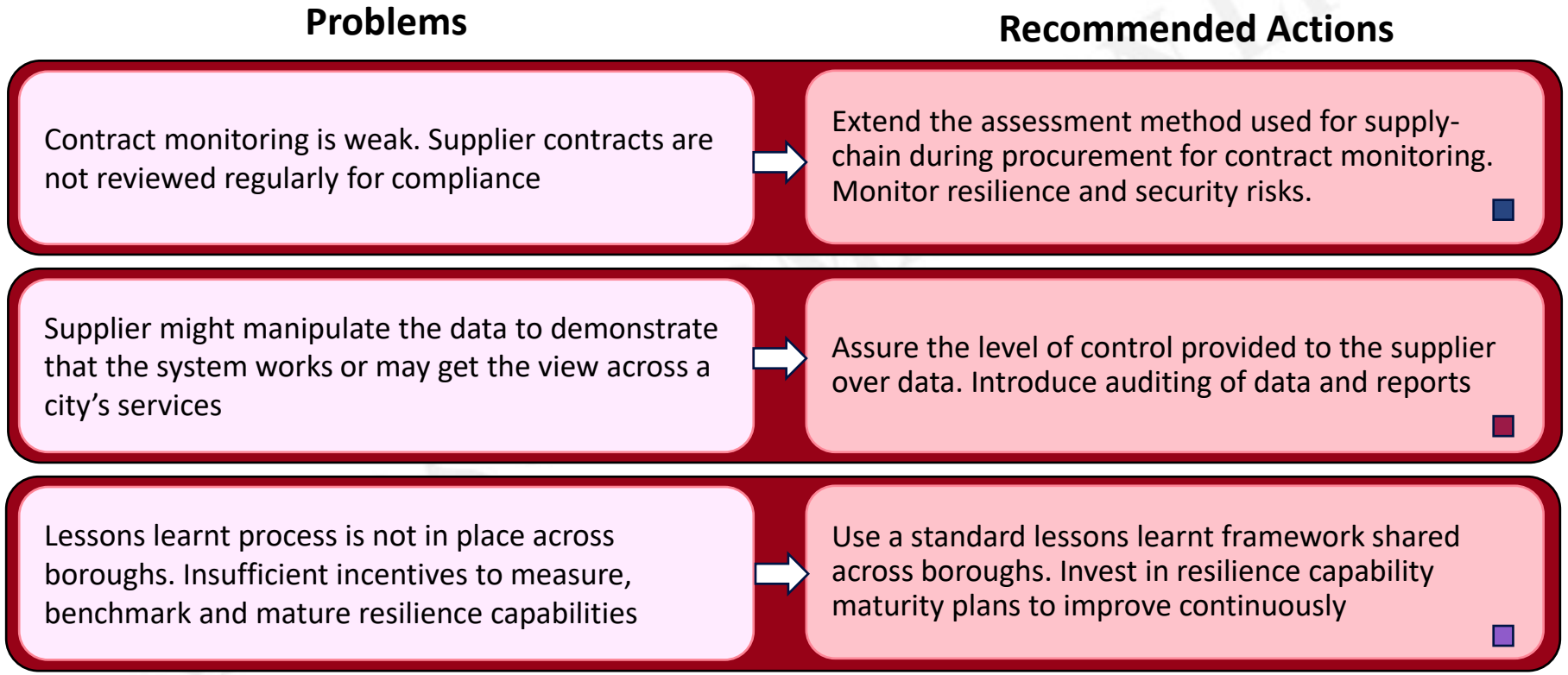
LOTI Procurement Step 4: Execute



Selected Sources (for the more complete set of references please see appendix):

- NCSC Secure Design Principles
- NCSC Cyber Assessment Framework
- Crown Commercial Service Technology Products 2
- IoTSF IoT Security Compliance Framework

LOTI Procurement Step 5: Manage



Selected Sources (for the more complete set of references please see appendix):

- NCSC Secure Design Principles
- NCSC Cyber Assessment Framework
- Crown Commercial Service Technology Products 2
- IoTSF IoT Security Compliance Framework

Summary of Recommended Actions

Risk Management

- Methodology and tools to assess connected service risks and liabilities in procurement life-cycle
- Involvement of right stakeholders upfront and governance across all procurement channels
- Methodology for proportionate and relevant resilience measures by design

Supplier Assessment

- Checklist of standards for compliance and best practices
- Methodology and tool for supplier assessment questionnaire
- Methodology to assess supplier responses holistically
- Supplier response gap analysis mapped to risk treatment plan

Contract Management

- Design service and contract performance criteria for resilience and security even in trials
- Methodology to monitor resilience and security risks across people, process, technology
- Review ongoing feasibility and efficiency of controls against required resilience

Service Assurance

- Methodology and tool to audit suppliers for compliance and level of control over data
- Design regular tests for resilience and supplier's view/use of data
- Changing landscape impact assessment methodology

Capability Development

- Process and tool to capture lessons learnt and continuous improvements
- Trainings on Smart Service resilience and procurement framework
- Extend research in discovery phase and educational trainings

5. Recommendations

5 Top Recommendations

1	**Refine operating model for smart service procurement**	Define changes to organizational structure, Roles, Responsibilities, processes, capabilities, people
2	**Guide with tool for smart service risk management in procurement**	Framework and tool for standard risk-based analysis for connected services and proportionate measures
3	**Resilience and security assessment guide with tool for smart services**	Resilience and security assessment best practice checklists based on mapped standards, mapping to risk management for connected impacts and liabilities
4	**Smart services Research and Training programme**	Research to capture and learn from similar global projects, mandatory quarterly training for awareness, training to create and implement recommended changes
5	**Supplier Awareness and Development programme for smart resilience**	Bring suppliers on board with resilience requirements for their platforms, partner with them, enable their capability development through awareness programmes

3 Quick win Actions

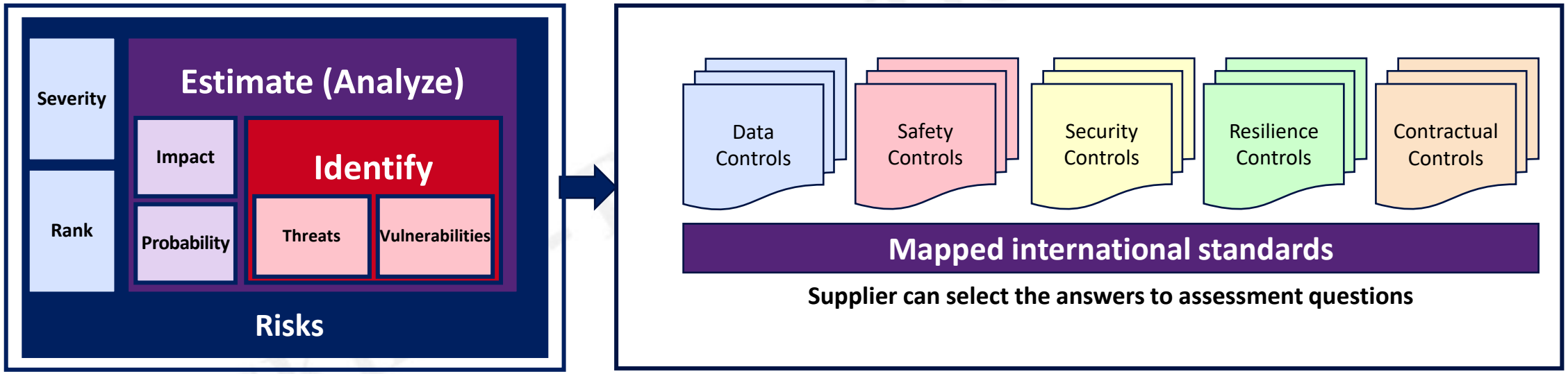
Basic Supplier Assessment Pilot

Refine operating model

Educational Training for smart service impacts

Quick win Action 1 - Basic Supplier Assessment Pilot

1.1 Create a prefilled pilot questionnaire associated with 10 steps of resilience



Basic Supplier Assessment Pilot…continued

Our Framework 10 steps of cyber resilience

Sample Questionnaire from our Service Resilience Capability Assessment Tool SR-CAT

Vendor Name:		xxx Ltd.					
Service Name:			Service name				Date
QUESTIONAIRE		**Standards / Compliance needs**	**Meets Requirement**	**Partially meets requirement**	**Does not meet requirement**	**Select Response**	**Pass/Fail/ Assess risks**
Step 1: Identify Current and Future Risk Scenarios							
1	Have you assessed the most probable and most severe (worst-case) scenarios of current service disruption?	NCSC CAF Dx, ENISA IoT security a point b, PAS 185/2017 section x, clauses ya, yb, yc	List of requirements / controls that are mapped from relevant industry standards	Manual input	State of not meeting the requirements	Partially meets requirement	Assess Risks

1.2 Create a risk treatment plan for residual risks based on supplier assessment gaps

1.3 Potentially merge this tool with any existing Crown / Spark procurement online assessment tools

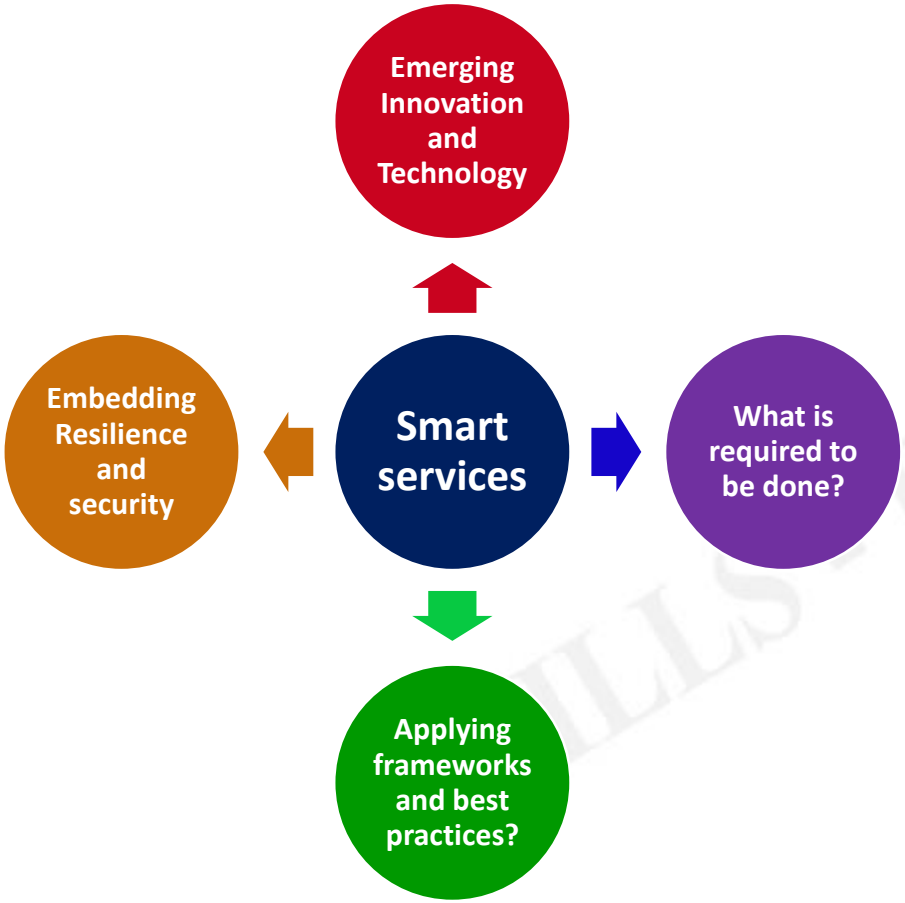
Quick win Action 2 – Refine processes and governance

1. Plan an iterative roadmap – "Who, what, where, how and when"
2. Identify and implement process improvements
3. Identify and implement governance changes
4. Share the practices across boroughs

Examples: 1) Change the process and governance to involve IT, Operations and service design in procurement discovery
2) Ensure governance checklists are signed off across all procurement channels

- Use tools such as cyber-insurance for further quick wins
- Facilitate and encourage knowledge sharing across smart city initiatives

Quick win Action 3 – Educational Training for smart service impacts



- Leverage thought leadership to get key messages across
- Understand existing standards and frameworks for smart city initiatives
- Improve supplier awareness
- Provide understanding of how to identify and adapt to the new ways of working
- Be able to identify smart service risks and liabilities
- Learning how to assure smart service resilience and security compliance

* We have the capability to tailor our trainings in collaboration with experts

Suggested Next steps

1

- Review by NCSC/CPNI/Crown
- Detailed write-up for suggested cyber-resilience measures to refine LOTI framework

2

- Update the cyber-resilience measures based on NCSC and CPNI guidelines to be published for smart city
- Incorporate into national procurement frameworks

3

- Create prioritized work-packages for quick wins
- Coordinate with other smart service initiatives from Central and local Governments in UK

6. Appendix

Our Team and Acknowledgements

Our Core Team of consultants from Skills-Formation Ltd

Meha Shukla: Founder
And Cyber Risk Management Consultant

Derek Tam: Digital Technologist

Acknowledgements

1. Eddie Copeland - LOTI
2. Jay Saggar – LOTI
3. Genta Hajri – LOTI
4. Tom – NCSC
5. Theo Blackwell – GLA

Special thanks to contributors in this project for their valuable insights

Key References

- NCSC Cyber Assessment Framework (CAF), https://www.ncsc.gov.uk/collection/caf
- Crown Commercial Service Spark DPS https://www.crowncommercial.gov.uk/agreements/RM6094
- Crown Commercial Service Technology Products 2 https://www.crowncommercial.gov.uk/agreements/RM3733
- https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice
- CPNI, “Smart Cities Specification For Establishing and Implementing A Security-Minded Approach”, https://www.cpni.gov.uk/system/files/documents/b7/db/CPNI%20-%20Smart%20cities.pdf
- CPNI, Protective security considerations, https://www.cpni.gov.uk/protective-mitigation
- UK Government, Code of Practice for consumer IoT security, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
- IoT Security Foundation, IoT Security Compliance Framework Release 2.1, https://www.iotsecurityfoundation.org/best-practice-guidelines/
- ETSI, Cyber Security for Consumer Internet of Things: Baseline Requirements, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- Enisa, Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
- NIST, Guide for Conducting Risk Assessments, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- NIST, Security and Privacy Controls for Federal Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- Infocomm Media Development Authority, Singapore, Consultation for IoT Cyber Security Guide, https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2019/consultation-for-iot-cyber-security-guide
- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), “Security Best PracticeGuidelines”, https://www.hkcert.org/f/guideline/262205/cc040767-fa07-4c87-aaa9-cdf46d4b92c6-DLFE-14203.pdf
- Mapping Security & Privacy in the Internet of Things https://iotsecuritymapping.uk/

About Skills-Formation Ltd

Who are we?

We are specialists in Smart Services Cyber Resilience for connected devices. We aim to enable the transformation of skills and capabilities to build resilient cities of the future. Our Mission is to Lead the way for global cyber resilience of connected smart services

What do we provide?

We are the creators of Service Resilience - Capability Assessment Tool SR-CAT, an assurance framework for 10 steps to cyber resilience

Why are we Different?

Our comprehensive range of services focus on integration with existing business processes, ease of adoption and cutting through complexity. Our unique market leading cost-effective solution will be reviewed with NCSC and is delivered in partnership with public, private, academia and standards body. We pride ourselves on our ability to contribute to the sustainable resilient global smart city initiatives and deliver a cutting-edge solution that meets the real-world needs of the security of important city services for the citizens.

THANK YOU

Email: uctzshu@ucl.ac.uk
www.skills-formation.com