2019 IEEE International Conference on Cyber Security 2019

Does the NIS implementation strategy effectively address cyber security risks in the UK?

Meha Shukla, PhD Candidate
Dawes Centre of Future Crimes, UCL,
London, UK

About the authors

Meha Shukla

PhD Candidate at
Jill Dando Institute
Department of
Security and Crime
Science
University College
London (UCL)
London, UK

Shane Johnson

Professor at
Jill Dando Institute
Department of Security
and Crime
Science
University College
London (UCL)
London, UK

Peter Jones

Professor at
Department of Civil,
Environment and
Geomatic Engineering
University College
London (UCL)
London, UK

Research sponsor: Dawes Centre for Future Crime at Jill Dando Institute UCL, London, UK

Summary of this Research

1. About the Research

This research explored how cyber security risks are managed across UK Critical National Infrastructure (CNI) sectors following implementation of the 2018 Networks and Information Security (NIS) legislation.

2. Method

Data gathered through Government reports and websites and interviews with 35 key stakeholders in CNI sectors was analyzed. Samples included organizations that are important to the Smarter London Together Roadmap.

3. Results

Key gaps were found in NIS implementation include cross-sector CNI service security measures, outcome-based regulatory assessments and holistic security. 10 recommendations have been provided to bridge these gaps.

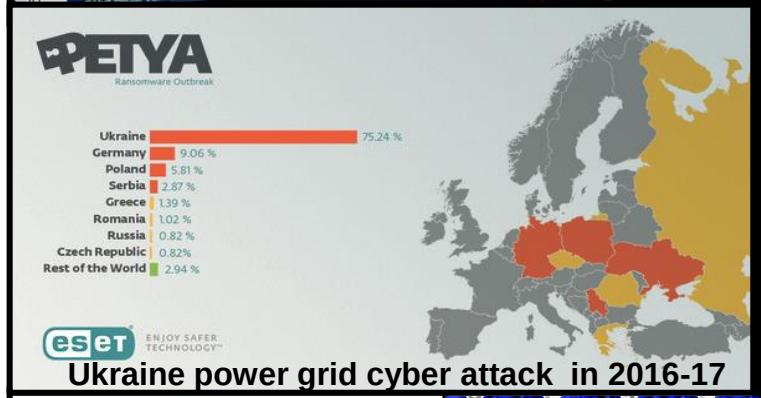
4. Conclusion

The NIS implementation strategy in the UK needs further alignment with its objectives, to effectively manage cyber risks in the UK. More effort is required in bringing a step-change in the cyber-security risk management capabilities of the CNI sectors which can also benefit smart London cybersecurity planning.

Background

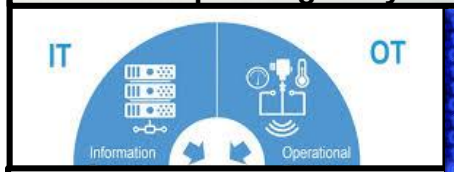
German rail attack in 2017

Wanna cry attack on UK hospitals in 2017



Ukraine power grid cyber attack in 2016-17

Atlanta water supply attack in 2018



- The global cyber security breaches so far make it clear that over and above the technology, an effective approach to deal with cyber security threats is to manage risk-based security of people and processes as is the case in a business transformation model
- Cyber security risk management involves understanding the critical business processes supporting the critical services and the underlying components, systems, networks, physical assets and personnel.

Note: IT – Information Technology, OT – Operational Technology

Introduction to NIS Directive

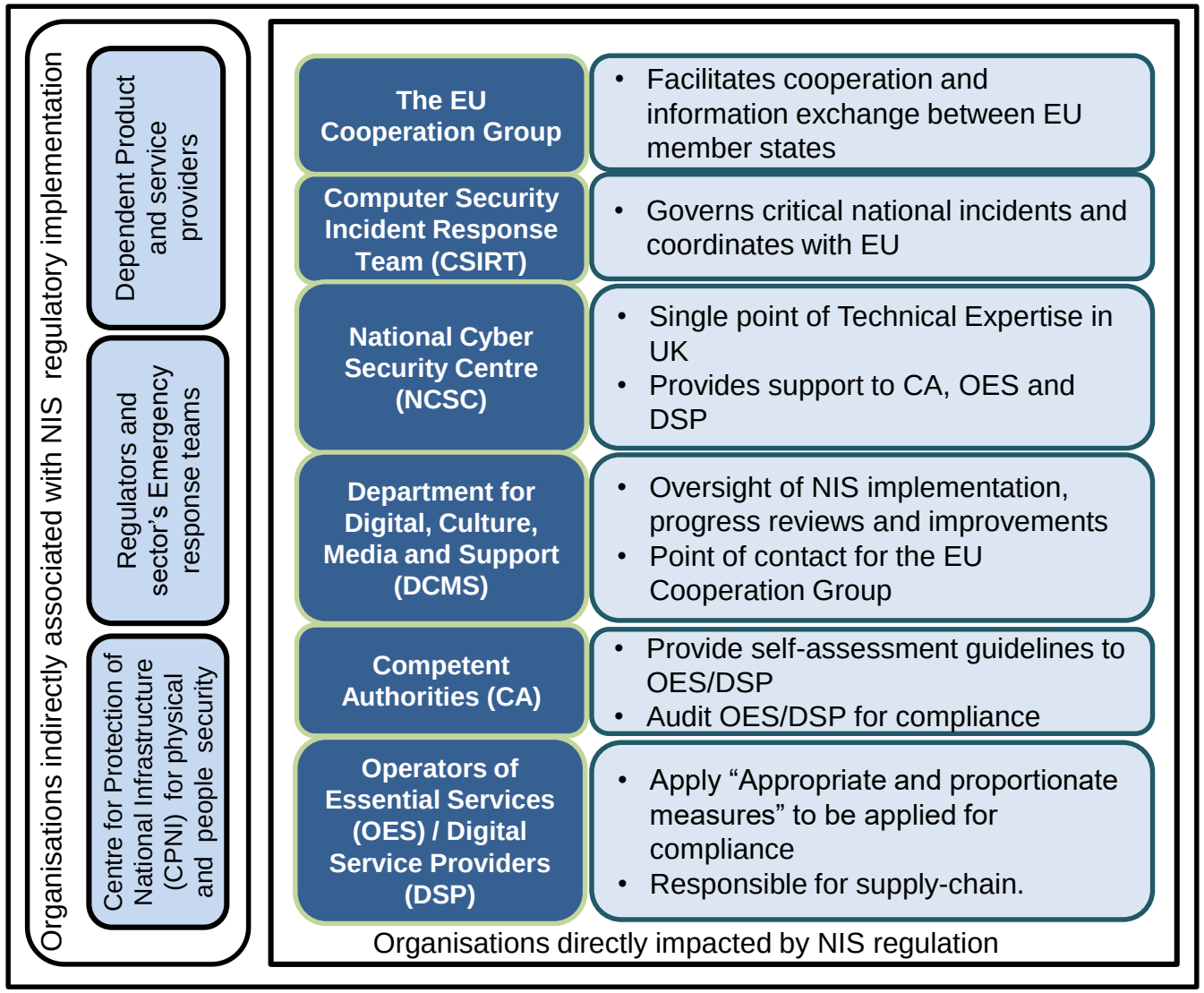
What is NIS?

- EU Directive on security of Network and Iinformation Systems (NIS) of Critical National Infrastructure (CNI)
- Adopted by the European Parliament in July 2016 and transposed to EU member states in 2018
- Penalties for non-compliance
- UK transposed the Directive into national law in May 2018

NIS Objectives

- Improve security levels and resilience of Operators of Essential Services(OES) and Digital Service Providers (DSP)
- Establish a forum to communicate between EU countries
- Provide a national and EU level legal framework for cyber risk management and notification of serious incidents.

NIS Implementation in the UK



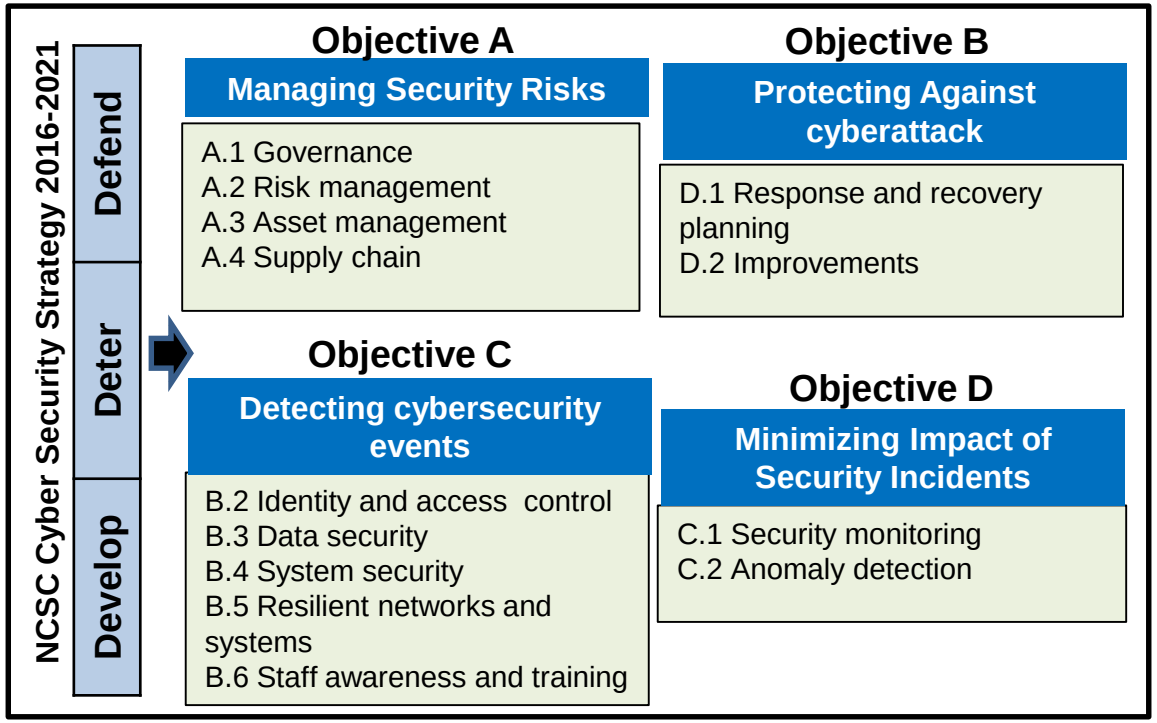
Organizations

- **Health and Social care**
- **Transport –air, maritime, road and rail**
- **Digital Service Providers**
- **Drinking Water Supply and Distribution**
- **Energy**
- **Digital Infrastructure**
- **Exempt sector – Banking and Finance**

CNI Sectors

Research Questions

This research was explored whether the NIS implementation strategy effectively addresses cyber security risks in the UK.



Cyber security risk management Capability Assessment framework (CAF) from National Cyber security Centre's (NCSC) – UK

Q- 1 Are there gaps in the current cyber security risk management framework under NIS legislation?

Q-2 Is the NIS directive's approach, aimed at bringing step change in the cyber security risk management across UK's CNI sectors, effective?

Q-3 How do points in a) and b) fit into the Smart London cyber security planning?

Research Questions

Method - Study of NIS Implementation process

Fig. 4. NIS regulatory compliance process

NIS Compliance Framework Diagram (IT Governance, 2018)

Sector-specific self-assessment tool/guidance by Competent Authority (CA)

Question

Questions

Questions

Self Assessment by Operators of Essential Service (OES)/ Digital Service Providers (DSP)

Sl	Gap Analysis	Impact Assessment
1	RED	Medium
2	AMBER	Medium
3	GREEN	Medium

Action plan for the identified gaps

Decision by CA on the compliance status post review and monitoring of the action plan

Feedback to National Cyber Security Centre (NCSC)

Feedback and reporting to Digital Culture Media and Services (DCMS)

Observations

- State-governed approach puts the liability on OES and DSP (including their supply chain)
- Flexibility lies in competent authorities deciding what are the appropriate and proportionate measures, organizations are developing a realistic action plan
- Framework is outcome driven and does not mandate how an organization must achieve those outcomes
- The approach encourages open, collaborative and iterative development
- Capabilities vary across sectors. Energy, DSP, road subsector (transport), water sector is are in formative stages

Measuring NIS Effectiveness

Research Questions

Q- 1 Are there gaps in the Cyber security risk management framework under NIS legislation?

Q-2 Is the NIS directive's approach, aimed at bringing step change in the cyber security risk management across UK's CNI sectors, effective?

Q-3 How do points in a) and b) fit into the Smart London cyber security planning?

Methods

Data Analysis

- 35 stakeholders from 30 organisations impacted by NIS and Smart London together plan identified as samples for the research. Data collected through interviews and reports

Case Study 1

- The current framework of a sample sector (Health) were compared with the NIS requirements provided by NCSC framework

Case Study 2

- The requirements for cyber security of non- CNI organizations within Smart London plan were compared against the NIS framework

Analysis - Current risk management activities and gaps in the NIS sectors were compared with NIS objectives and a few best practices in Finance sector

Results

Gaps were found in implementation strategy, governance, people, process, technology and improvement approach

Self-assessment checklist does not effectively meet the NIS objective of outcome-based risk management

Integration of NCSC CAF into the design cycle of smart city plans can be beneficial

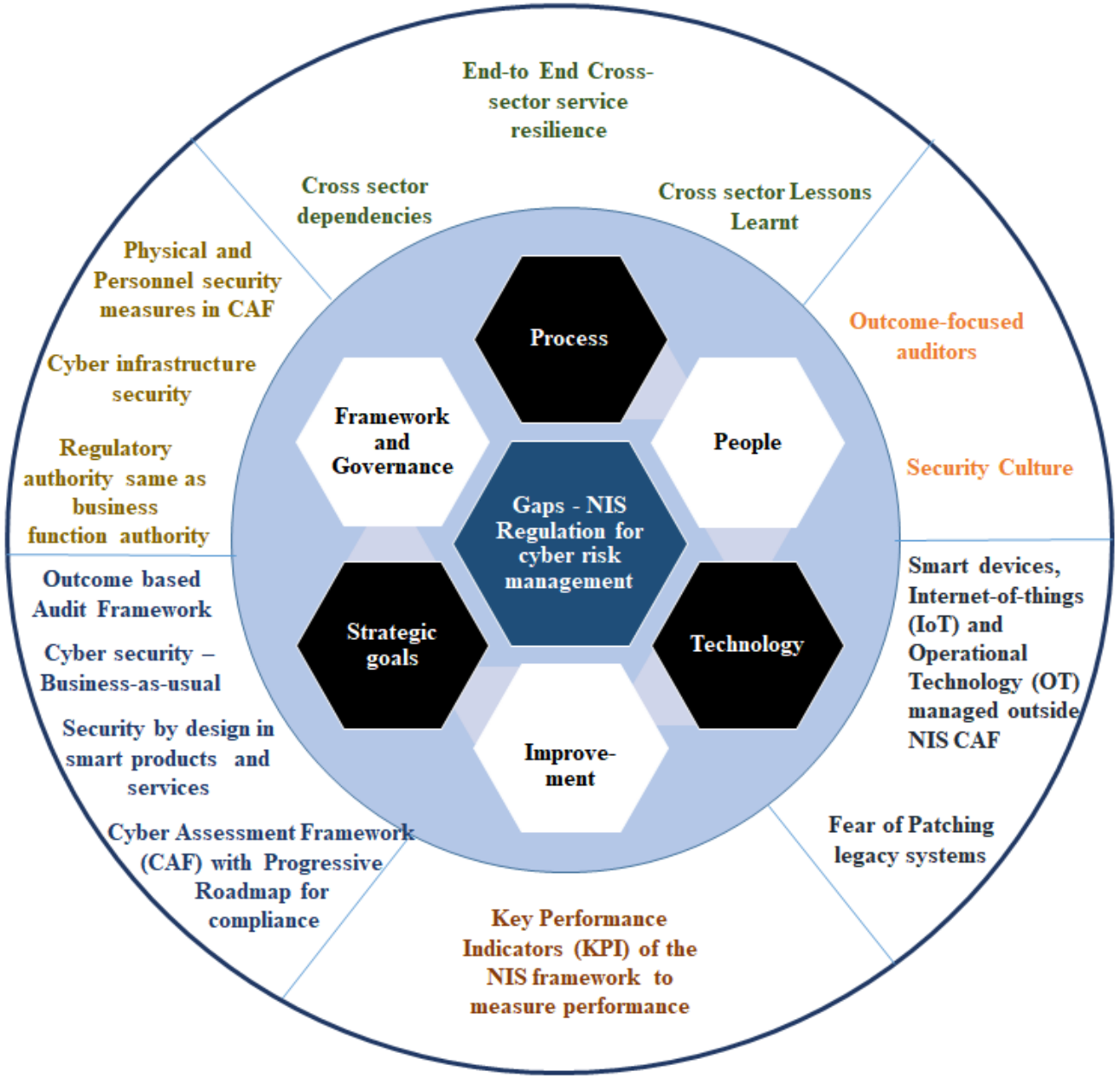
Summary of Benefits and Gaps

Benefits

- NIS implementation follows a collaborative approach to improve service resilience
- NIS provides a method to deal with the evolving nature of cyber security risk mitigations without continuous amendments to the legislation, and therefore, is scalable and sustainable.
- NIS principles could be adopted by the other non-CNI organizations in the UK
- Integration of U.S. NIST and EU NIS frameworks could be a starting point for a global framework for holistic security and risk management

Limitation of this research

This research is a snapshot in time
(May 2018 to Aug 2018)



Recommendations and Conclusion

Recommendations to improve NIS effectiveness

1	Refine National Cyber Security Center (NCSC) Capability Assessment Framework (CAF) and NIS governance across cyber, physical and personnel security	6	Include Internet-of-things (IoT), Operational Technology (OT), smart products and smart services in NCSC CAF
2	Outcome-based NIS audit framework oversight and governance to be developed	7	Define Key Performance Indicators (KPIs) by May 2019 to gather data and manage NIS performance
3	Setup cross-disciplinary outcome based audit teams from various business functions	8	Integrate NIS framework with safety, quality, risk management and business assurance frameworks
4	NCSC CAF to include Cross-sector End-to-End holistic service resilience, Competent Authority (CA) forums to share cross-sector lessons learnt with the industry	9	CAF Indicators of Good Practice (IGP) and smart city plans to include cyber security-as-Business-as-usual (BAU) approach within the engineering life-cycle (including design)
5	NIS Audits to assess effectiveness of key controls of top business and service assurance risks with an outcome-based approach	10	Create multiple levels of CAF outcomes and target capability roadmap for Operators of Essential Services (OES)/ Digital Service Providers (DSP)

Key Takeaways

1. The NIS implementation strategy in the UK needs further alignment with its objectives

2. More effort is required in bringing a step-change in the cyber-security risk management capabilities of the CNI sectors

Recommendations for further Research

UK NIS enforcement compared with other EU countries integration points for cyber security frameworks between UK and other leading countries

2. Cyber security strategies and frameworks of smart cities, products and services compared to London

Thank you

We express our gratitude and thanks to Dawes Institute of Future Crime at UCL (Sponsor), all the stakeholders (the list below), Maria Bada (University of Oxford); Prof Brian Collins(UCL); Barry Emerson (CIO NHSE London); Chris Hurran (RSES); Dr. Saira Ghafur and Martin Guy (Imperial College London); and Marco Franken and Alexandra Luck (consultants).

1) Isabel Bonachera Martin, EU Cyber Security Regulatory Policy, Department for Digital, Culture, Media and Sports (DCMS)
2) Department of Health and Social Care (DHSC)
3) Theo Blackwell, Chief Digital Officer of London, GLA
4) Department of Transport (DfT)
5) Simon Onyons, Finance Conduct Authority(FCA)
6) Nick Davey, Payment System Regulator (PSR)
7) Centre for Protection of National Infrastructure (CPNI)
8) The Office of Gas and Electricity Markets (OfGem)
9) National Health Service (NHS) England
10) Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Deutschland
11) David Tait, Civil Aviation authority (CAA)
12) Nick Swanson, City Hall, GLA
13) London Fire Brigade
14) London Metropolitan Police
15) Steve Burton, Transport for London (TfL)
16) Johnny Schute, James Walker, Ian Maxwell, Office of Rail and
Road (ORR)
17) Hitachi Vantara
18) Toby Gould, London Resilience Group
19) Graham Lane, City Hall, GLA
20) Imperial College Healthcare
21) North West London NHS Foundation Trust - CNWL
22) NHS Digital
23) British Standards Institute (BSI)
24) Network Rail
25) Defra, Drinking Water Inspectorate(DWI)
26) Business, Energy and Industrial Strategy (BEIS)
27) Office of Communications (OfCom)
28) Bank of England(BoE)
29) Information Commissioner's office (ICO)
30) Highways England

Note: Stakeholders names have been included only where stakeholder's permission was given to do so.

APPENDIX B – EXPLANATION OF TERMS

BAU – Business-as-usual BoE – Bank of England
BEIS - Business, Energy and Industrial Strategy
BSI - British Standards Institute
CA – Competent Authority
CAA - Civil Aviation Authority
CAF – Capability Assessment Framework
CAP - Civil Aviation Publication
CAV - Connected and Automated Vehicles
CBEST – Cyber threat assurance framework
CCT - Cyber Compliance Team
CDO – Chief Digital Officer of London
CNI – Critical National Infrastructure
CPNI - Centre for Protection of National Infrastructure
CSIRT - Computer Security Incident Response Team
CQC - Care Quality Commission
DCMS – Department for Digital, Culture, Media and Support
Defra - Department for Environment, Food and Rural Affairs
DfT - Department of Transport
DHSDSP – Digital Service Providers
DSPT - Data Protection and Security Toolkit
DWI - Drinking Water Inspectorate
C – Department of Health
ENISA - European Network and Information Systems Agency
EU – European Union
FCA - Finance Conduct Authority
GCHQ - Government Communications Headquarters
GDPR - General Data Protection Regulation
GLA – Greater London Authority
HSE - Health and Safety
ICO - Information Commissioner's Office
ICS – Industrial Control Systems
IGP – Indicators of Good Practice
IoT – Internet of Things
ISO – Institute of Standardization
IT – Information Technology
KPI - Key Performance Indicators
NATO - North Atlantic Treaty Organization
NCSC – National Cyber Security Centre
NHS - National Health Service
NII - National Information Infrastructure
NIS – Networks and Information Security
NIST - National Institute of Standards and Technology
OES – Operators of Essential Services
OfCom –Office of Communications
OfGem - Office of Gas and Electricity Markets
OfWat – Office of water services
ORR – Office of Rail and Road
OT – Operational Technology
PAC - Public Accounts Committee
PAS - Publicly Available Specification
PDCA – Plan-Do-Check-Act
SCADA - Supervisory Control and Data Acquisition
TfL – Transport for London
UCL – University College London UKRN - UK Regulators Network