Operational Excellence in Practice

Session Chair:

Steve Sadler
Technology Strategy Lead, TSA

THE TEC EVOLUTION
Connecting communities and enriching lives

Session Contributors

Paul Shead

Member of the Sector Risk and Innovation Group

Stuart Ellis

Member of the Sector Risk and Innovation Group

David Hammond

Member of the Sector Risk and Innovation Group

Operational Excellence – what it means to TSA

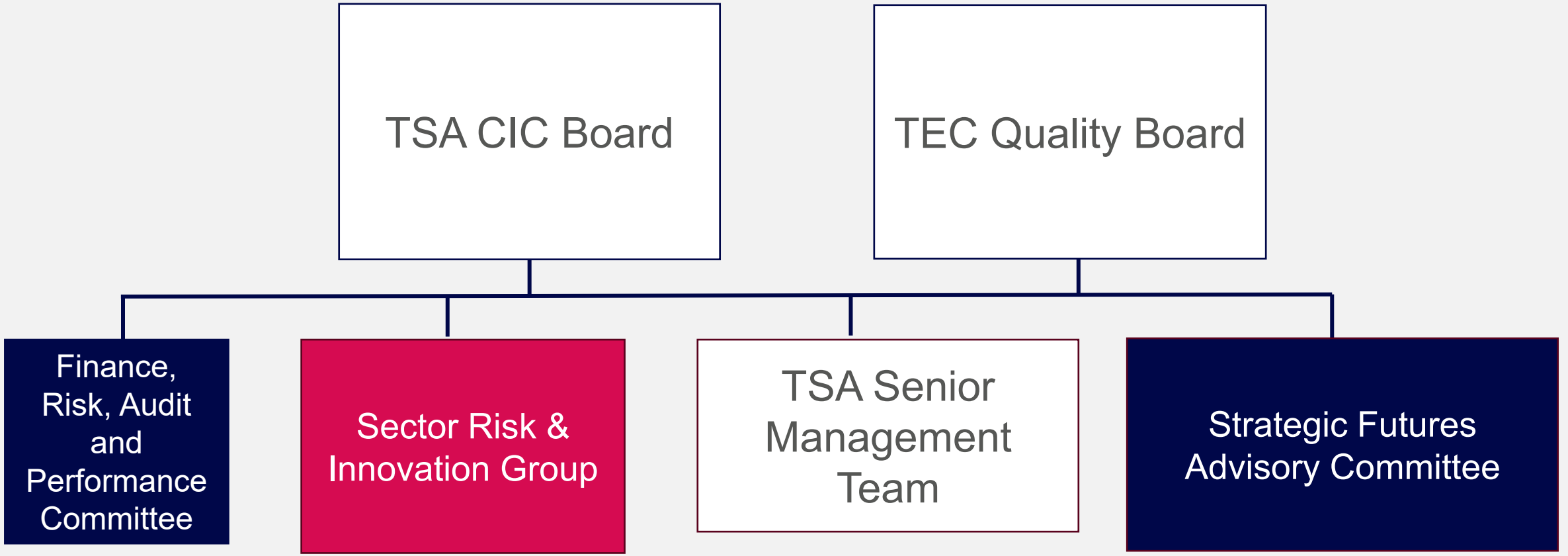
The pursuit of continuous improvement, efficiency and quality in everything we do, so that we can:

Maximise the value for our members and people who draw on care and support services

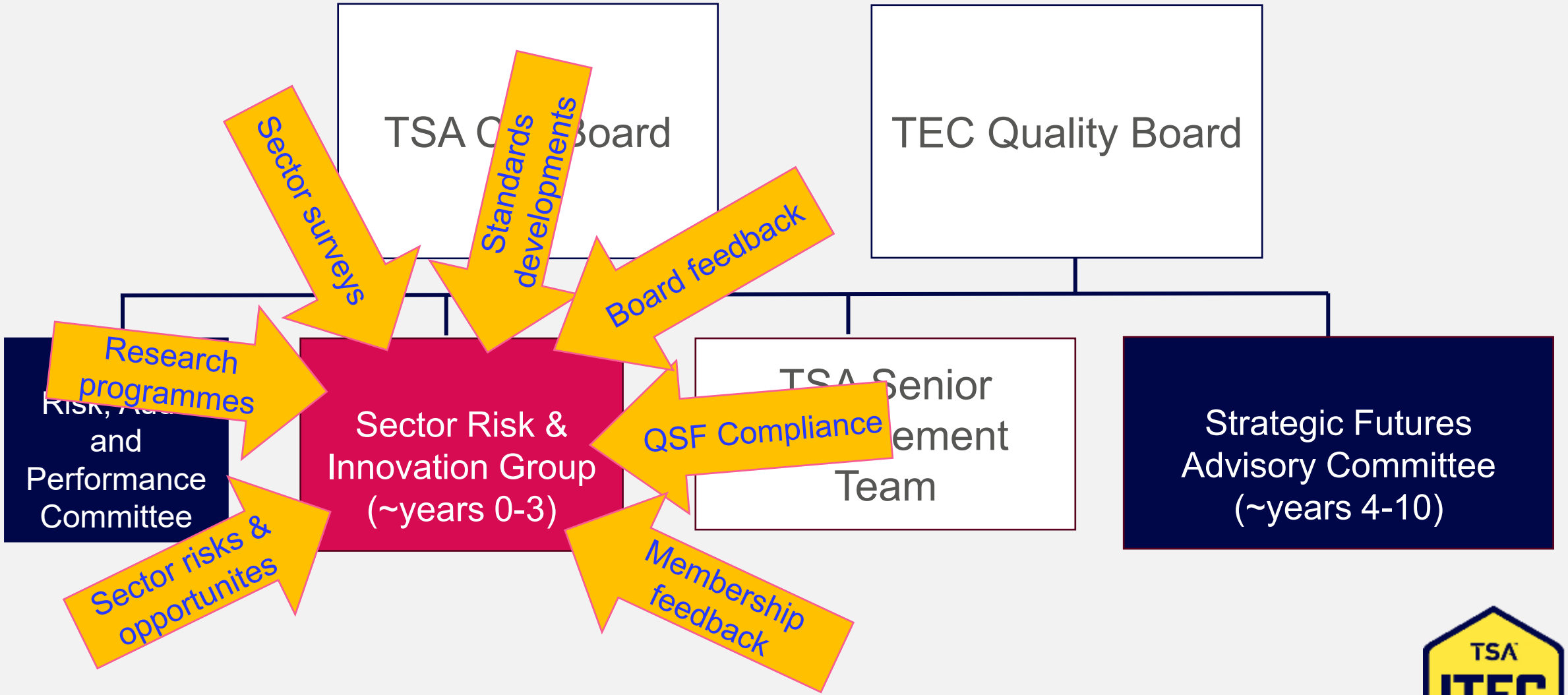
Take the key opportunities for TEC to make a difference

This needs clarity of goals, commitment to change and delivery processes that are fair and accountable.

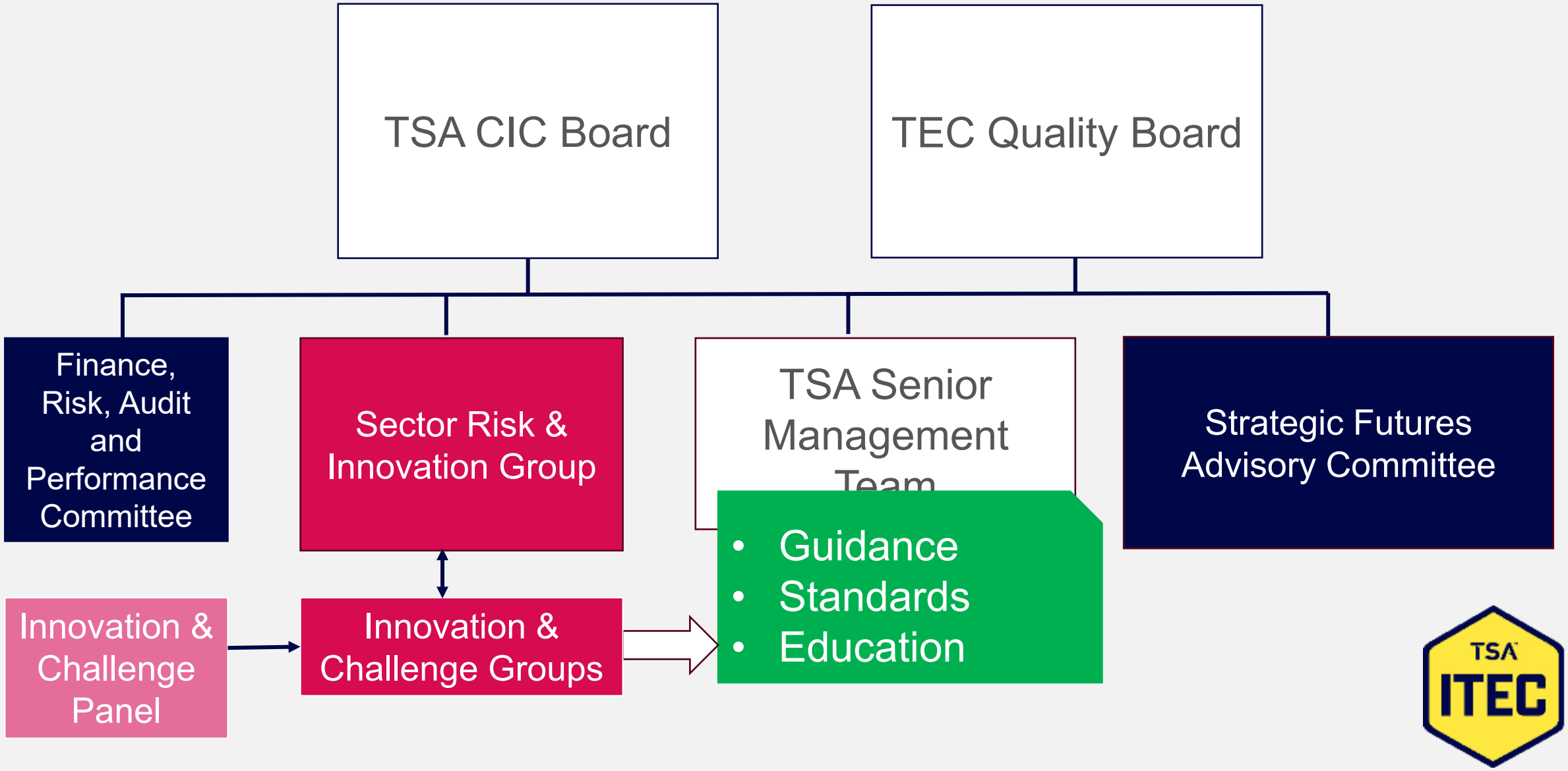
Organising for Operational Excellence



Organising for Operational Excellence



Organising for Operational Excellence



Sector Risk and Innovation Group (SRIG)

Alyson Scurfield
Chair of SRIG and
CEO of TSA

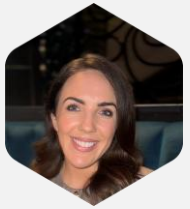
Rich Amos
Lived Experience Adviser

Paul Berney
Principal Associate, TSA

Gary Clark
Technical Director, Careium

Stuart Cole
Independent Living Services
Manager, Mole Valley

Stuart Ellis
Head of IT, Taking Care



Charlotte Findlay
Head of Membership Services, TSA

David Hammond
Chief Executive Officer,
Chiptech

Helen Loveday
Head of Quality and
Improvement, TEC Quality

Stuart Parsons
Director Consulting Services, CGI

Rupert Lawrence
Head of Medequip Connect

Steve Sadler
Technology Strategist, TSA

Paul Shead
Managing Director, Enovation

SELECT OR DEFINE STANDARDS FOR INTEROPERABILITY & INTEGRATION OF TEC

Paul Shead
Managing Director, Enovation UK

Member of the Sector Risk and Innovation Group (SRIG)

THE TEC EVOLUTION

Connecting communities and enriching lives

With thanks to the following organisations, who contributed greatly to the initial development of the interoperability matrix

TSA ITEC

Taking Care
Part of AXA Health

chiptech

Chubb
POWERED BY APi GROUP

Anthropos

TIS

everon™

essence smartcare

access
freedom to do more

enovation
care to connect

CSL

careium®

TeleAlarm®
SWISS TECHNOLOGY

possum
life enhancing solutions

astraline
a partnership for living

legrand® | care

appello

iotcomms.io

SKYRESPONSE

Tunstall

IoT Solutions Group

ASTER GROUP

Select or define standards for interoperability & integration of TEC

Objective:
To address the need for ‘seamless operation’, with the intention to guide service providers in deploying digital services more effectively and reliably.

Completed

- Interoperability matrix published and regularly updated
  https://www.tsa-voice.org.uk/digital-shift/resources/interoperability-matrix/
- Verified by the TSA with monitoring service providers
- Definitions of “interoperability” and “integration” provided
- Currently focused on digital devices to ARC platforms, confirming the protocols used by
  - Dispersed alarms
  - Scheme alarms
  - GPS alarms
  - Scheme IP converters

Digital Devices	Device Type	<ARC platform supplier 1>			<ARC platform supplier 2>		
		Protocol(s)	ARC Confirmed	Customer Verified	Protocol(s)	ARC Confirmed	Customer Verified
<Manufacturer & Model 1>	eg Dispersed Alarm	TS50134-9/SCAIP	☑	☐	TS50134-9/SCAIP/ SIPS	☑	☑
<Manufacturer & Model 2>		SCAIP/TS50134-9	☑	☑	SCAIP	☑	☐

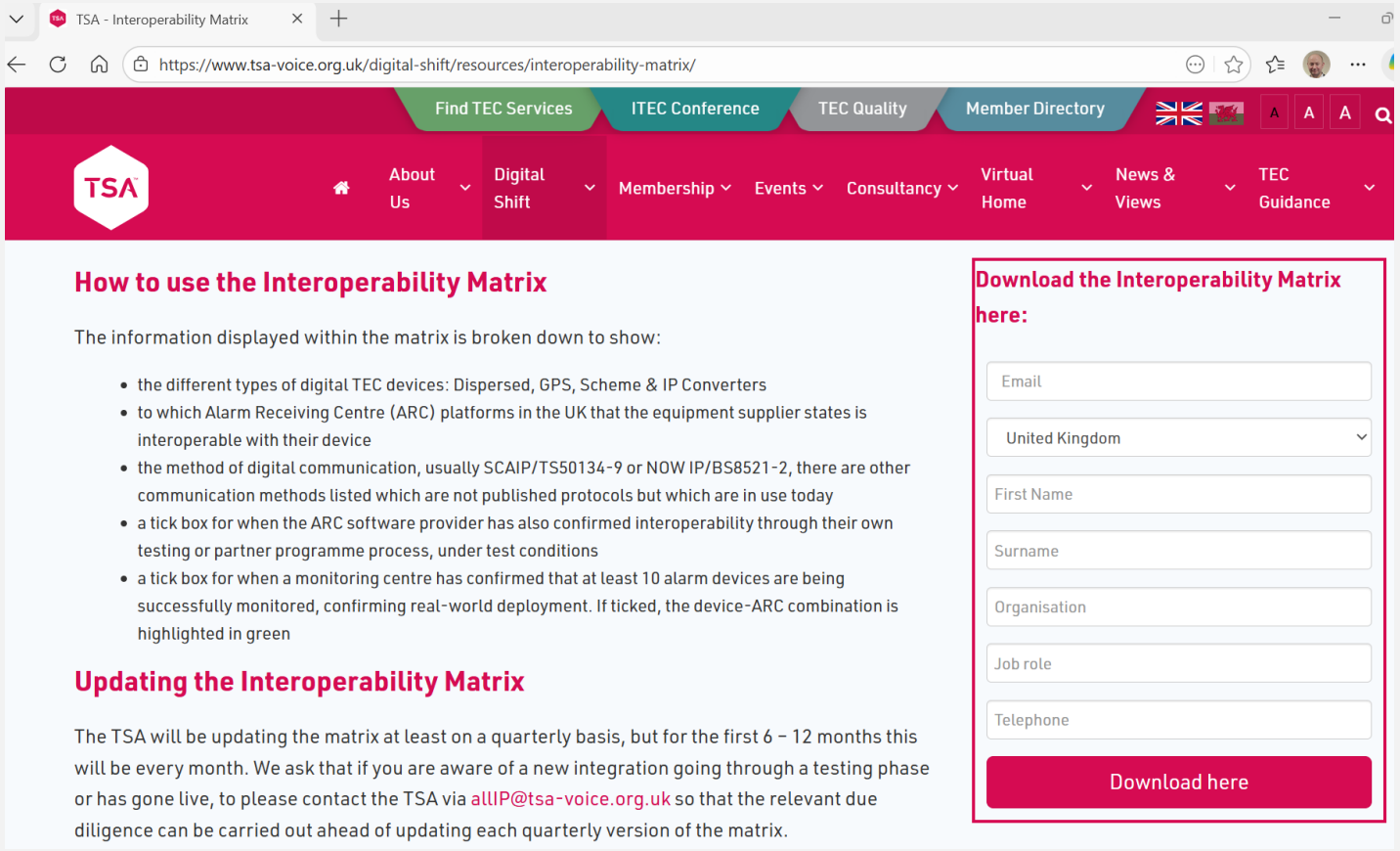
Next steps

- Scope review, considering wider interoperability of
  - proactive/preventative devices and platforms with ARCs
  - data exchange between different systems
  - we are seeking volunteers who are experts in these fields!

Suppliers: How to update your matrix entry

Download the current Interoperability Matrix here
https://www.tsa-voice.org.uk/digital-shift/resources/interoperability-matrix/

Change requests can be emailed to:
allip@tsa-voice.org.uk



TSA ITEC

TEC-SPECIFIC CYBER RISKS & INCIDENT MANAGEMENT

Stuart Ellis
Head of IT, Taking Care

Member of the Sector Risk and Innovation Group (SRIG)

THE TEC EVOLUTION

Connecting communities and enriching lives

Innovation and Challenge Group Members

Sonia Calder
2ic-care

Helen Loveday
TEC Quality

Emma Quest
TSA

Andreas Fransson
Careium

Terry Meredith
iOnline

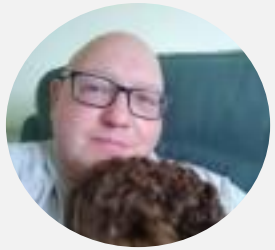
Herman Thom
iOnline

Will Edgell
NRS

Chris Pugh
TEC Quality

Emily White
Chiptech

Richard Keyse
2ic-care



Darren Cotton
Tunstall

David Jack
Tunstall

Cyber Risks: What we've learned..

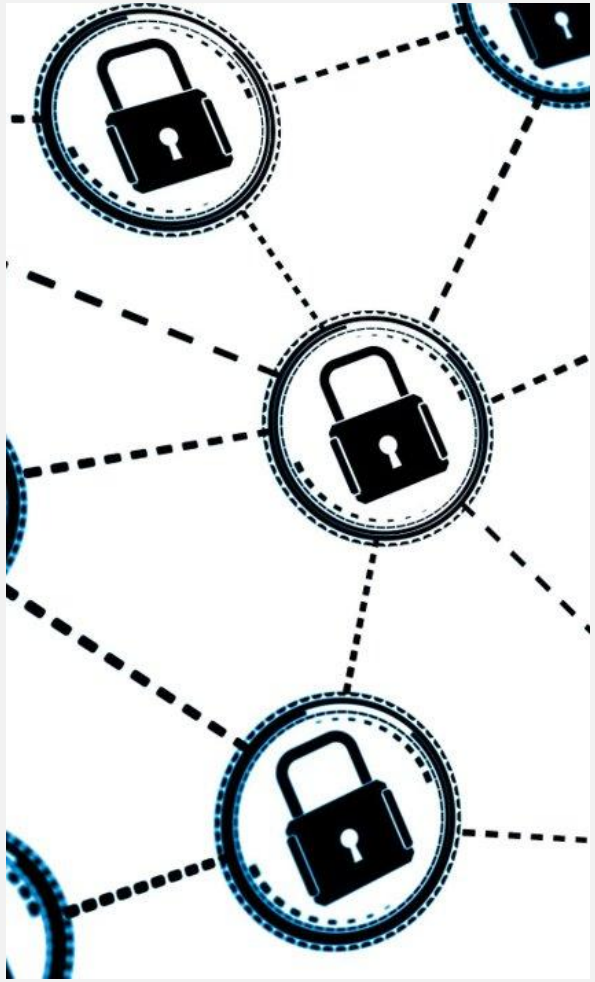
Cyber risk in TEC is real and growing

The SRIG cyber work set out to identify TEC cyber risks and publish mitigation guidance, and to improve incident management guidance

Current learning: most risks are not "TEC-unique cyber" they are familiar cyber risks with direct impact on TEC service uptime and safety outcomes

TEC's increasing reliance on cloud and SaaS platforms shapes its evolving cyber risk profile

The emphasis therefore shifts to 'Security by Design' embedded into the TEC industry through signposting to existing standards, training, and QSF guidance



Cyber Risks

Common Cyber Risks in TEC
Most cyber risks in TEC are common threats like connectivity loss, cloud outages, and compromised credentials from phishing, etc

Integration of Cybersecurity
Embedding Security by Design into TEC resilience ensures cybersecurity is part of architectural and operational decisions

Focus on Service Continuity
Cyber risk management in TEC prioritises service uptime, safety, beyond niche IT concerns

Pragmatic Cyber Risk Approach
TEC organisations should establish baseline controls, through risk management and prepare effective incident responses integrated with business continuity and DR

Do I need Cyber Insurance?

QSF had stated:

“Demonstrate awareness of the risks presented by cyber-attacks, and that through informed decisions, a risk-based approach to cyber security and insurance has been undertaken.”

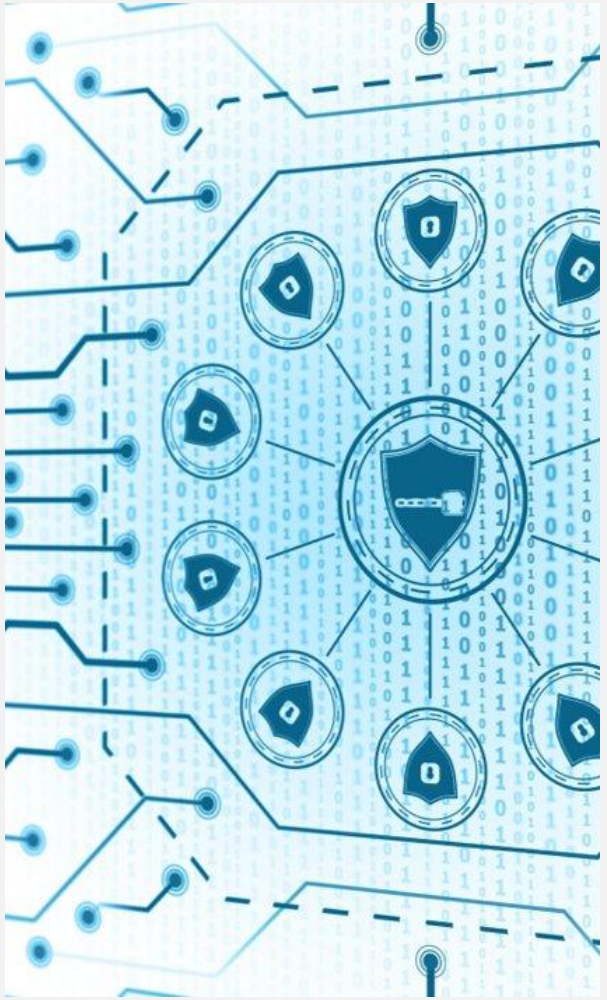
Cyber insurance can help manage financial impact, but it does not prevent incidents.

Insurers increasingly expect baseline controls (e.g. Cyber Essentials) and tested incident response plans to remain valid

Policies should include both first-party and third-party cover, such as:

1. Incident response and forensic support
2. Business interruption and system recovery
3. Data protection, regulatory and legal liabilities

Cyber insurance should be considered part of a broader resilience and incident management approach, alongside business continuity.



Changes to Cyber Essentials

What's changing in Cyber Essentials v3.3

From 27th April 2026:

- **MFA becomes mandatory across all user accounts**
- **Mandatory protections for cloud services**
- **Stronger Evidence requirements**

QSF Cyber Standards

QSF Compliant

NHS DSPT

Advanced Compliance

SOC 2

Future Addition

Outstanding Compliance

NIST

Future Addition

The Message for TEC Industry

1

Resilience by Design

Embed cybersecurity into resilience by design to ensure service availability & user safety from the start

2

Supply Chain Assurance

Assure supply chain resilience and compliance with service uptime and SLAs

3

Incident Preparedness

Prepare for cyber incidents through planning, exercises, and coordinated technical/operational and communication responses

4

Outcome Focus

Focus on outcomes like service availability, Cyber Insurance & Certification, drives risk-based cybersecurity maturity

STANDARDS FOR RESILIENCE OF SERVICES & SYSTEMS

David Hammond
CEO, Chiptech

Member of the Sector Risk and Innovation Group (SRIG)

THE TEC EVOLUTION
Connecting communities and enriching lives

Innovation and Challenge Group Members

Richard Bailey
Mobius Networks

Julian Edge
Chiptech

Richard Hosier
Everon

Ian Nicholson
Enovation

Max Stevens
CSL

Rebecca Simmons
TEC Cymru

“Just go digital” – The challenge

Over 30 years we operated in an analogue world. We were comfortable with
One copper line, One path, One dependency, One clear failure mode.

As digital started to scale, it was clear that resilience work as a sector was needed.
New challenges included:

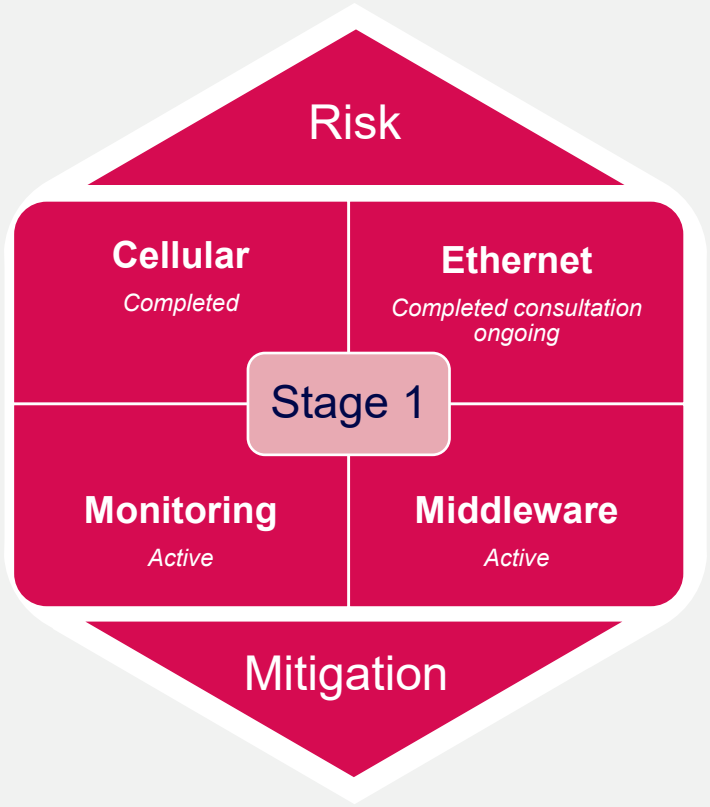
Shared consumer broadband, Power dependent routers
SIM provisioning, Cellular roaming
DNS layers, Cyber exposure
Interoperability challenges
and more:

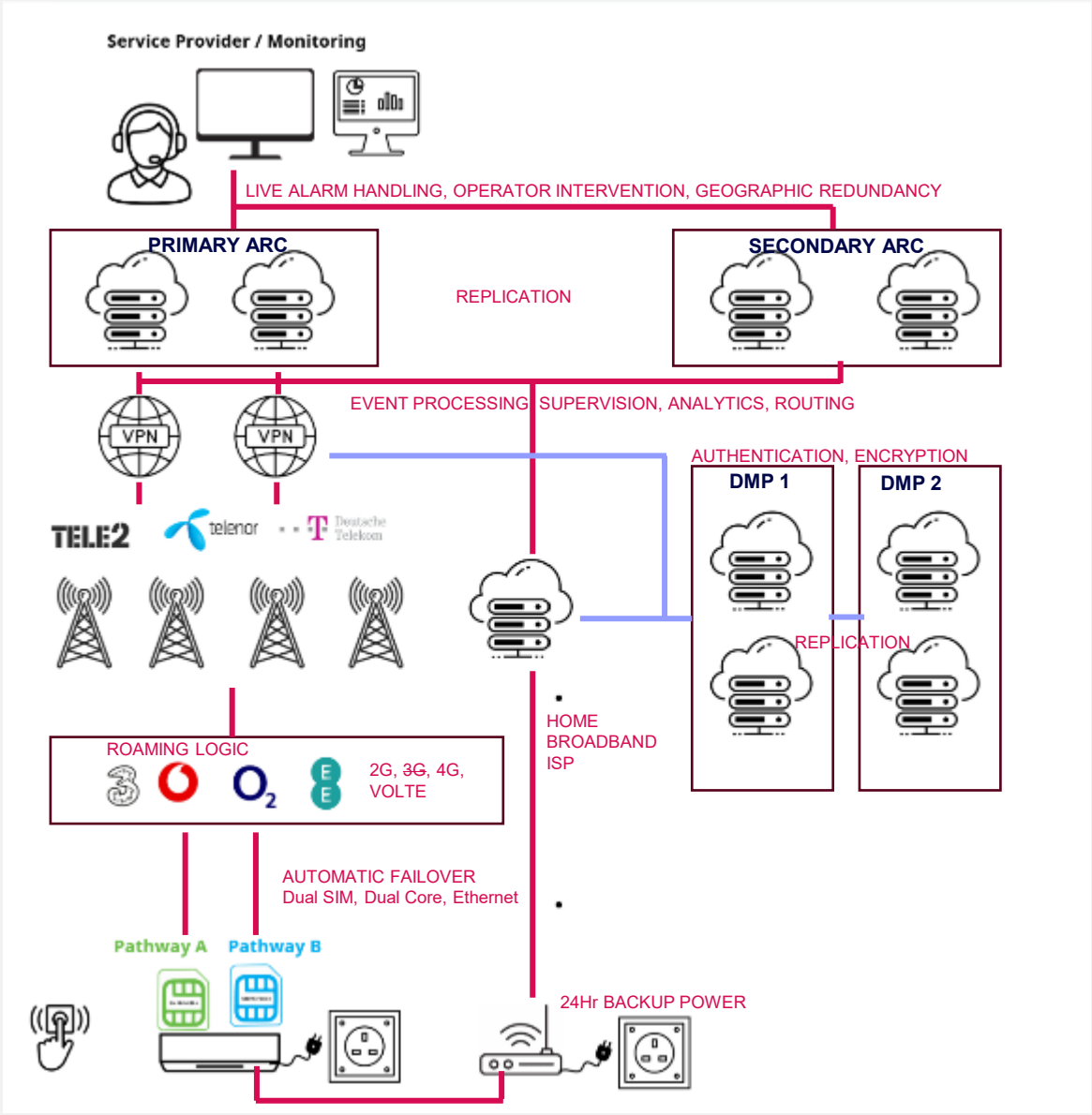
SRIG 2.4 Risk and Resilience Goals:

To identify, guide and advise on system level risks and resilience
To bridge information between commissioners, service providers, ARCs, Comms and Equipment providers
To create a place for shared knowledge
To guide QSF
To guide on resilience measures for our industry's future in big data

Project and Process

- Identified real-world failure modes over “the system”
- Multi-stakeholder recruitment with relevant expertise
- Documented risk with impact and mitigation
- Provide guidance documentation
- Tested through consultation
- QSF guidance





Cellular Output

We have completed our first Cellular work which includes 2 papers, intended for:
Commissioners, Design Authorities, Service Providers, Equipment providers, Comms providers and ARC's

Managing Risks of Cellular Connectivity in Technology Enabled Care

Key Recommendations for Safe Use of Cellular

- Connectivity in TEC
- Cellular communication in TEC - What is it and How does it work?
- Risks Identified and Mitigating Actions
- Network Reliability Risks
- Device and SIM Functionality Risks
- Configuration and Setup Risks
- Communication and Accountability
- Capacity and Scalability Risks
- Network Sunsets and Futureproofing

Detailed Risk Assessments

Risks Identified

- Detailed Risk Assessments, Impact Descriptions, Technical Mitigation and Service Mitigation
- Terms of Reference and Acronym Glossary

Highlights from the Cellular Work
From Assumed Reliability to Designed Resilience

01

Connectivity loss should be visible, not silent

02

Cyber governance is explicit, not implied

03

Cellular Resilience spans device, ARC and comms layer

04

Dual path resilience is a baseline requirement

Cellular Risk Mitigation for Life Critical Alarm Services

Highlights for:

Commissioners

Digital resilience written into the requirements

- Mandate dual communication pathways as a baseline procurement requirement
- Specify 4G/VoLTE capability, prohibit 3G-only device procurement
- Require professional M2M SIMs only, never consumer SIMs
- Apply a personalised risk-based approach per BS8684:2024
- Require joint commissioning sign-off across equipment, monitoring and service providers

Cellular Risk Mitigation for Life Critical Alarm Services

Manufactures & SIM/Comms providers

Digital TEC Engineered and Interoperable resilience

- Provision M2M SIMs with no usage caps, no suspension triggers, and static IP where required
- Disclose roaming partner agreements and any single network dependencies transparently
- Give service providers advance notice of APN, IP, or VPN changes
- Design for dual-path communication Implement intelligent roaming algorithms based on real-world performance
- Ensure 4G/VoLTE support and OTA firmware update capability
- Use industrial-grade tamper-resistant SIM holders

Cellular Risk Mitigation for Life Critical Alarm Services

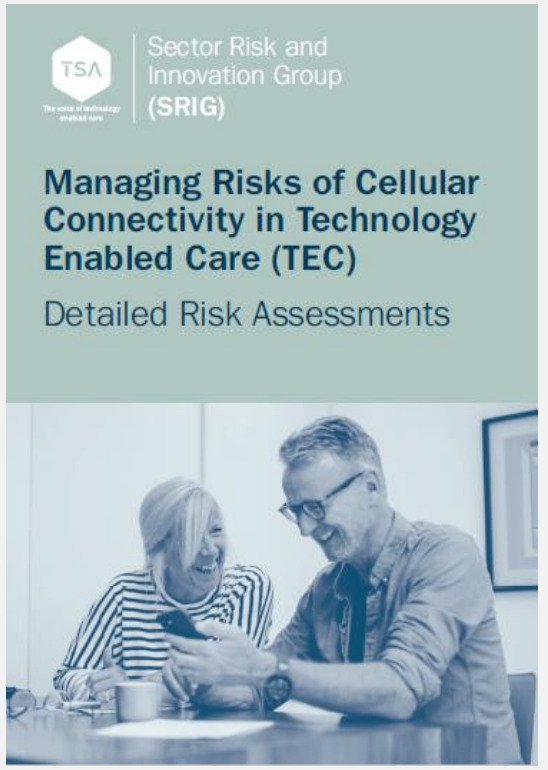
ARC's

Digital TEC Resilience - managing fleet behaviour

- Implement network-level alerting for clusters of failures, not just individual device alerts
- Configure telephony to accept inbound calls from international and roaming SIM number ranges
- Register both SIM numbers for dual-core devices in the ARC databuild
- Capacity-test infrastructure for post-outage data flood scenarios with traffic prioritisation
- Maintain RACI defined escalation routes to all communication providers including out-of-hours contacts

Managing Risks of Cellular Connectivity in Technology Enabled Care (TEC)

A TSA Member resource, that will be emailed to all members on Wednesday 18 March



The SRIG Future Road Map

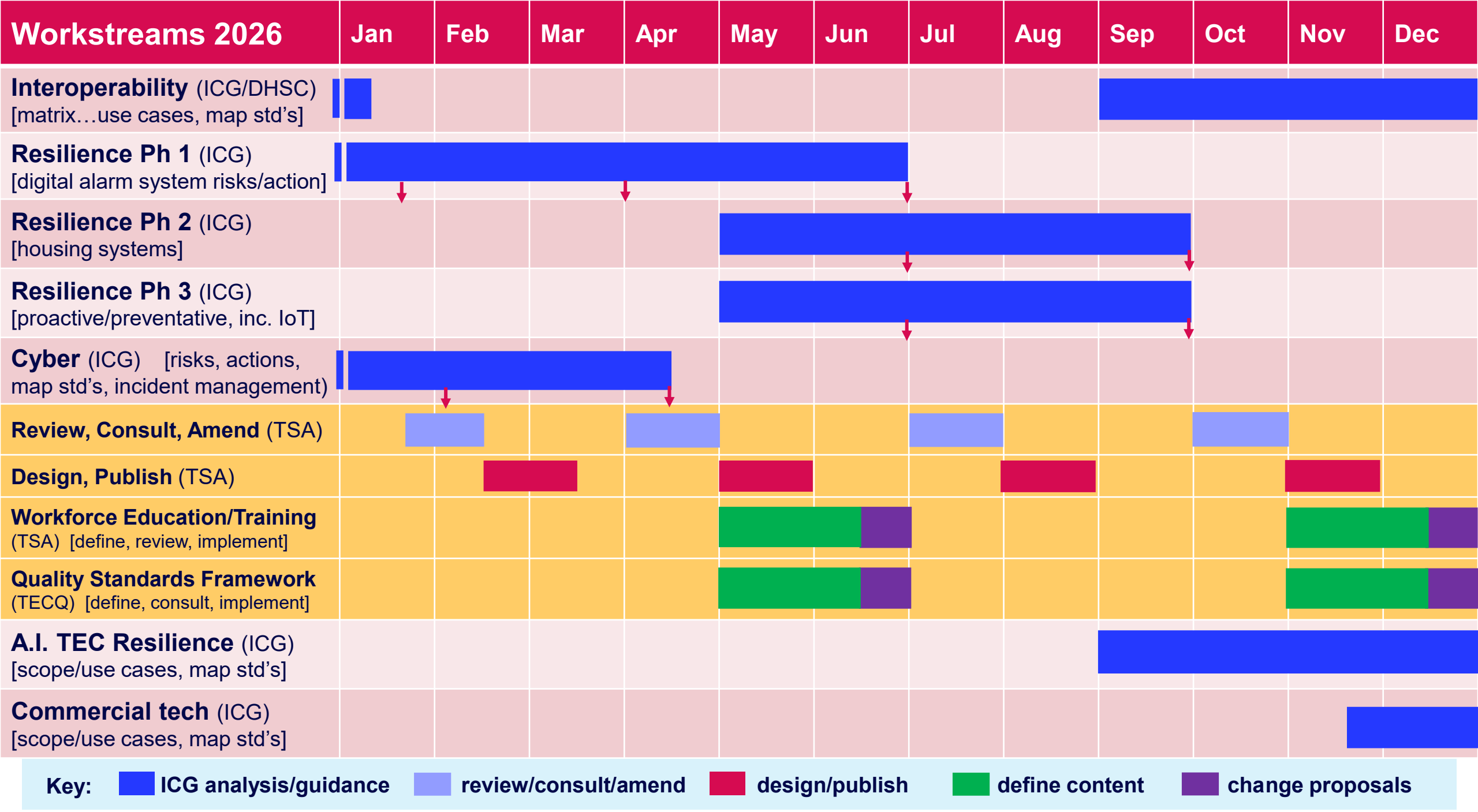
Steve Sadler
Technology Strategy Lead, TSA

Member of the Sector Risk and Innovation Group (SRIG)

THE TEC EVOLUTION
Connecting communities and enriching lives

2026 Workstreams

Resilience of Digital Alarm Systems Digital communications ARCs and Middleware Sensors, Alarms	to June'26
Resilience of Digital Housing Systems	May to Sept'26
Resilience of Proactive & Preventative TEC	May to Sept'26
A.I. Resilience in TEC	Sept'26 onwards
Interoperability across TEC	Sept'26 onwards
Commercial & Consumer Technologies in TEC	Nov'26 onwards


Workstreams 2026
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Interoperability (ICG/DHSC)
[matrix…use cases, map std's]
Resilience Ph 1 (ICG)
[digital alarm system risks/action]
Resilience Ph 2 (ICG)
[housing systems]
Resilience Ph 3 (ICG)
[proactive/preventative, inc. IoT]
Cyber (ICG) [risks, actions, map std's, incident management)
Review, Consult, Amend (TSA)
Design, Publish (TSA)
Workforce Education/Training (TSA) [define, review, implement]
Quality Standards Framework (TECQ) [define, consult, implement]
A.I. TEC Resilience (ICG)
[scope/use cases, map std's]
Commercial tech (ICG)
[scope/use cases, map std's]
Key:
ICG analysis/guidance
review/consult/amend
design/publish
define content
change proposals

Please get involved

TEC Quality

aico

HOLDEN GRANGE LTD
MONITORING SERVICES

Celebrating Excellence

QSF Certified 2025 - 2026

ATTENTIVE
Telecare Technologies

n-able
Part of Norse Group

Edinburgh Health and Social Care Partnership

dsp

FREQUENCY PRECISION®

telecom design

careBUILDER®

evondos group

GBR Digital Health Solutions

iONLINE
Connected Networks

Organisations on their QSF journey

ZINTOUCH
care.connect.protect

TEC Quality

Milton Keynes City Council

Careline Care

SCUTUM

Circadacare

ventro
FIRE COMPLIANCE

nationwide careservices
empowering people to live their lives

HOME SAFEGUARD
From East Devon District Council

ENS

Swindon Borough Council

Durham County Council

livity life

S.E.A LTD
Part of the S.E.A GROUP

MySense™

nobi

MEDEQUIP Connect

Panel Q&A

Paul Shead

Member of the Sector Risk and Innovation Group

Stuart Ellis

Member of the Sector Risk and Innovation Group

David Hammond

Member of the Sector Risk and Innovation Group

Thank You

www.tsa-voice.org.uk

#ITEC2026