TSA iTEC 25

TRANSFORMING LiVES THROUGH DIGITAL INNOVATION

The International Technology Enabled Care Conference. Unlocking insights. Building knowledge. Improving outcomes.

TSA™

STANDARDS FOR RESILIENCE OF SERVICES & SYSTEMS

David Hammond
CEO, Chiptech

Member of the Sector Risk and Innovation Group (SRIG)

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

Standards for Resilience of Services and Systems

Objective:

To risk assess the resilience of TEC systems, and sub-systems and how they impact services and to provide guidance on risk mitigation covering both technology and service.

Where we find that supporting information is not adequate, resilience guidance will either be produced and revised along with a revised Risk measurement.

Complete:

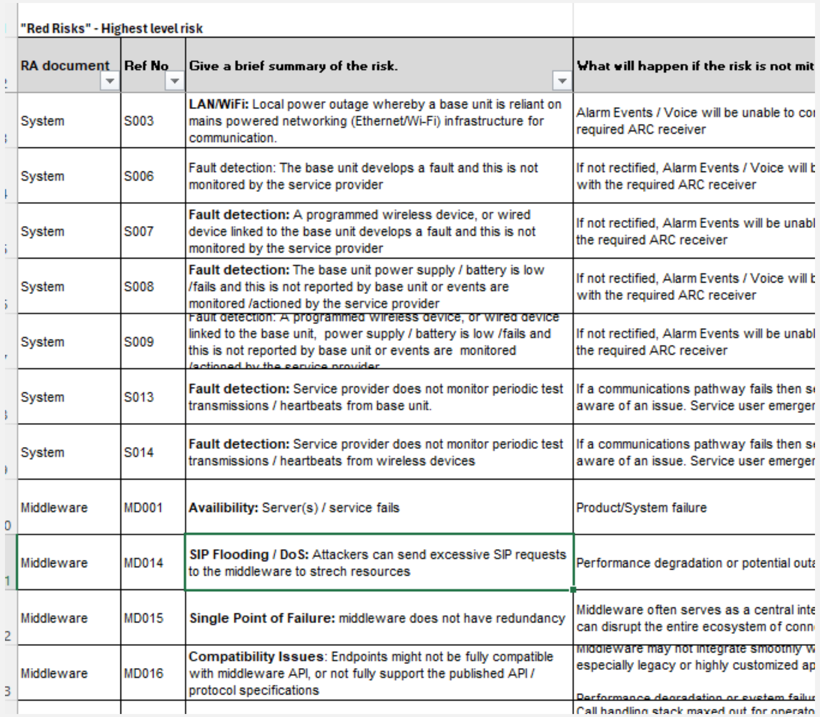
- Build experienced ICG team to support the project
- Conduct a full deep dive risk assessment of TEC Systems covering
  - *End to End Systems*
  - *Telecare – Independent Living*
  - *Telecare – Group Living*
  - *Cellular*
  - *WIFI/Ethernet*
  - *Monitoring*
  - *Middleware*
- Identify and Prioritise 'Red' risks

ICG Team	
Steve Saddler	TSA Technology Strategist
Rebecca Simmons	TEC Cymru Senior Project Manager
Richard Hosier	Everon Head of Product Development
Max Stevens	CSL Head of Telecare IOT
Ian Nicholson	Enovation Head of Technical Services
Richard Bailey	Mobius Senior Healthcare Sales
Julian Edge	Chiptech Head of Technical

Standards for Resilience of Services and Systems

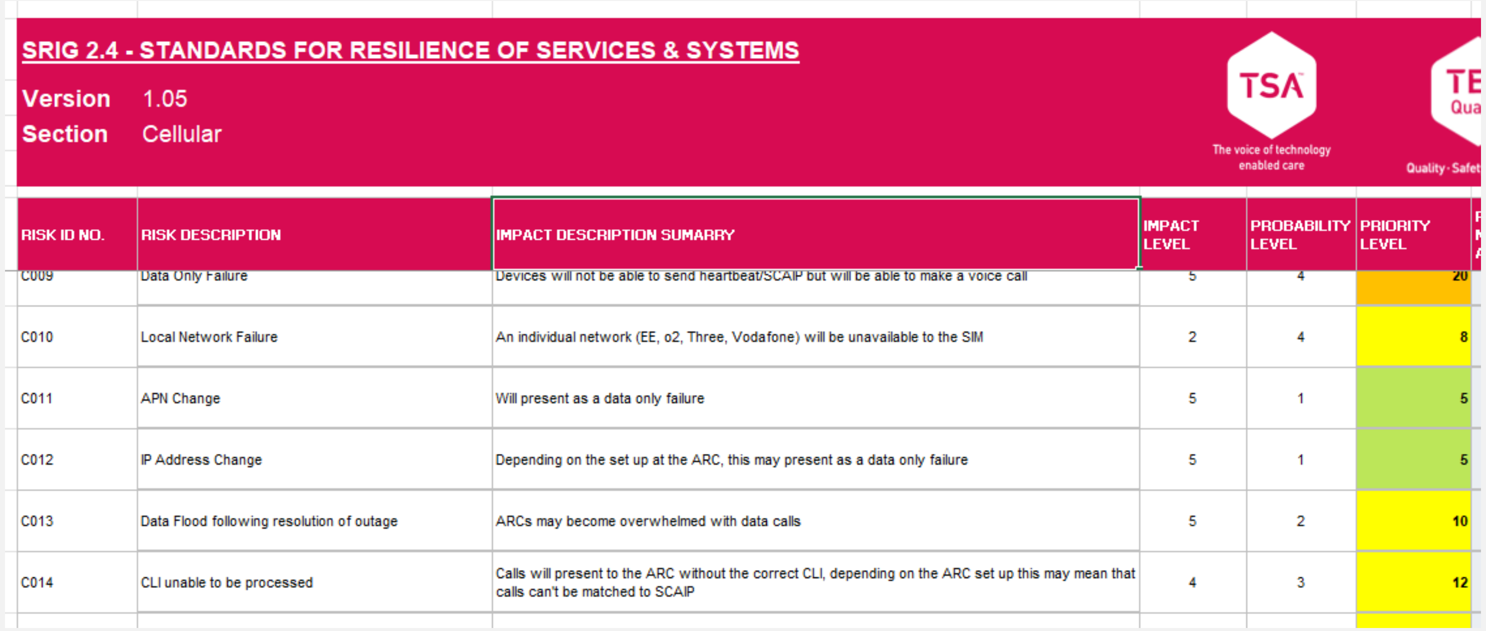
Complete:

- The team have identified >300 risks within the exercise.
- All risks highlight the importance of our QSF and also the importance of the work being carried out
- From this 300, 20 risks have been highlighted as High which are being prioritised.



"Red Risks" - Highest level risk

RA document	Ref No	Give a brief summary of the risk.	What will happen if the risk is not mit
System	S003	**LAN/WiFi:** Local power outage whereby a base unit is reliant on mains powered networking (Ethernet/Wi-Fi) infrastructure for communication.	Alarm Events / Voice will be unable to co required ARC receiver
System	S006	Fault detection: The base unit develops a fault and this is not monitored by the service provider	If not rectified, Alarm Events / Voice will b with the required ARC receiver
System	S007	**Fault detection:** A programmed wireless device, or wired device linked to the base unit develops a fault and this is not monitored by the service provider	If not rectified, Alarm Events will be unabl the required ARC receiver
System	S008	**Fault detection:** The base unit power supply / battery is low /fails and this is not reported by base unit or events are monitored /actioned by the service provider	If not rectified, Alarm Events / Voice will b with the required ARC receiver
System	S009	Fault detection: A programmed wireless device, or wired device linked to the base unit, power supply / battery is low /fails and this is not reported by base unit or events are monitored /actioned by the service provider	If not rectified, Alarm Events will be unabl the required ARC receiver
System	S013	**Fault detection:** Service provider does not monitor periodic test transmissions / heartbeats from base unit.	If a communications pathway fails then s aware of an issue. Service user emerger
System	S014	**Fault detection:** Service provider does not monitor periodic test transmissions / heartbeats from wireless devices	If a communications pathway fails then s aware of an issue. Service user emerger
Middleware	MD001	**Availibility:** Server(s) / service fails	Product/System failure
Middleware	MD014	**SIP Flooding / DoS:** Attackers can send excessive SIP requests to the middleware to strech resources	Performance degradation or potential outa
Middleware	MD015	**Single Point of Failure:** middleware does not have redundancy	Middleware often serves as a central inte can disrupt the entire ecosystem of conn
Middleware	MD016	**Compatibility Issues**: Endpoints might not be fully compatible with middleware API, or not fully support the published API / protocol specifications	Middleware may not integrate smoothly w especially legacy or highly customized ap Performance degradation or system failu
			Call handling stack maxed out for operato



SRIG 2.4 - STANDARDS FOR RESILIENCE OF SERVICES & SYSTEMS

Version 1.05

Section Cellular

The voice of technology enabled care

Quality · Safet

RISK ID NO.	RISK DESCRIPTION	IMPACT DESCRIPTION SUMARRY	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL
C009	Data Only Failure	Devices will not be able to send heartbeat/SCAIP but will be able to make a voice call	5	4	20
C010	Local Network Failure	An individual network (EE, o2, Three, Vodafone) will be unavailable to the SIM	2	4	8
C011	APN Change	Will present as a data only failure	5	1	5
C012	IP Address Change	Depending on the set up at the ARC, this may present as a data only failure	5	1	5
C013	Data Flood following resolution of outage	ARCs may become overwhelmed with data calls	5	2	10
C014	CLI unable to be processed	Calls will present to the ARC without the correct CLI, depending on the ARC set up this may mean that calls can't be matched to SCAIP	4	3	12

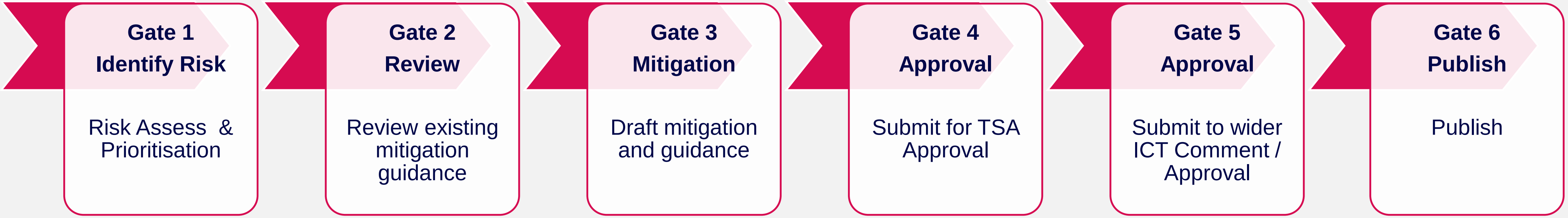
Standards for Resilience of Services and Systems

Ongoing

- Complete Risk Mitigation and guidance Documentation. Guidance to cover both Technical and Service Provision.
- Regularly update and maintain resilience guidance and standards for TEC systems and products.
- Identify and recommend further work required

Planned

- Publish resilience guidance and standards
- Review and update Service Resilience standards to complement new guidelines
- Develop training and tool recommendations for commissioners and providers to assess risks and apply mitigation strategies
- Define critical resilience metrics and propose amendments to the QSF
- Create RACI (Responsible, Accountable, Consulted, Informed) tools and guidance for system failures
- Widen Scope for IOT, Predictive/Preventative and AI based Systems
- Propose frequency for ongoing inclusion of risks and re-assessment exercise



Gate 1
Identify Risk
Risk Assess & Prioritisation

Gate 2
Review
Review existing mitigation guidance

Gate 3
Mitigation
Draft mitigation and guidance

Gate 4
Approval
Submit for TSA Approval

Gate 5
Approval
Submit to wider ICT Comment / Approval

Gate 6
Publish
Publish