The Resilience of TEC Monitoring Services

Author:
Steve Sadler, Head of Technology Strategy, TSA

The Resilience of TEC Monitoring Services
Version 2.5
6th December 2022

The Resilience of TEC Monitoring Services

Forenote: terminology

In this document, the term 'ARC' (Alarm Receiving Centre) has been replaced with 'TEC Monitoring Services'. Recently, the role of ARCs (now TEC Monitoring Services) has evolved. They now provide both reactive and proactive services - the change in terminology is to reflect this role and the services provided more accurately – TSA will refer to ARCs as 'TEC Monitoring Services' with immediate effect.

Special Interest Group 008 Objectives

The objectives of this Special Interest Group (SIG) are to identify key parameters that determine service availability, reliability, and data security, and to embed these as service measures in a tiered compliance framework in a manner that is an accessible indicator of service delivery and resilience for customers and commissioners.

This document aims to provide companion guidelines to the TEC Monitoring Services Resilience standards derived by SIG8

The SIG 008 standards highlight *WHAT* needs to be achieved by TEC Monitoring Services and systems, particularly in terms of data protection & security, availability and maximum tolerable down times.

These guidelines provide the first level of information on *HOW* to achieve these standards.

It is recognised that the guidelines should not delve into the individual architectures or processes that are relevant to the various suppliers of technology and services, and this supports the intention of providing only that first level of information which can be abstracted from individual solutions. The specific nature of individual service or technology solutions will only be employed where needed as examples, and where supplier approval has been obtained.

Special Interest Group 008 Work Programme

- SIG 008 has successfully identified a set of key measures and hence the candidate standards for resilience. These relate primarily to system availability (downtime) and security, and they are discussed below.
- The concept of service 'tiers' has been introduced, to differentiate between service types and their distinctive requirements. The following service definitions and example use cases apply:
    - **Reactive** (Priority 1): Real-time, life-critical call handling, including telecare alarms, smoke detectors, fall detectors
    - **Proactive** (Priority 2): Personalised outbound welfare check calls, medication reminders, and activities of daily living monitoring, all in response to a care plan
    - **Preventative** (Priority 3): Wellbeing apps, health questionnaires, advisory outreach services to a population of vulnerable people at risk

- A period of consultation with service providers and technology suppliers also resulted in a set of queries, which have been addressed. Here, the primary concern related to the sector's ability to meet any new standards in the short-term, with a request for a phasing-in of quality compliance requirements, to allow time for product and service developments.

Quality Levels Explained

Currently, when an organisation is audited and found to have achieved all the necessary requirements, they are rated as "Compliant", and this is the same for all organisations. However, we have experienced that some organisations go over and above the "minimum" requirements and we intend to introduce a process that recognises this fact. As we introduce the later phases of the TEC Monitoring Services Resilience standards, we will also start to recognise those organisations that truly strive for excellence. However, this must be based on higher quality, or higher degrees of safety, other than those levels currently in the QSF.

Therefore, the TEC Monitoring Services Resilience standards also introduce the concept of different levels of service 'quality level': "Compliant", "Advanced Compliance" and "Outstanding Compliance". The intention is that these quality levels will provide the means of easy comparison of services by commissioning customers and users, and they will be introduced as a full package of higher-level requirements in September 2023.

Proposed Quality Requirements and Phasing

It was identified that we need to allow time for organisations to prepare for these new standards, so a phased introduction has been agreed upon. A summary of the implementation phases can be seen below, followed by a further, more detailed explanation:

Phase	Date effective in QSF	Description
Zero	September 2021	Service Fitness for Intended Purpose
1	September 2022	Data Protection & Security standards
2	September 2023	Service Platform Availability
		- Availability of TEC Monitoring Service
		- Maximum Tolerable Downtime
		Quality Rating System Introduced
3	September 2024	Outfield equipment standards & measures published

Phase Zero – Fitness for Intended Purpose

This 'phase zero' aims to establish the basic principles that will underpin quality requirements. It examines the readiness of service providers for managing the resilience of their services.

This phase also acts as a 'lead-in' period for the application and measurement of the technical requirements that come later.

The basic principles reflect the Service Providers' understanding of the challenges that need to be addressed in providing suitably resilient services, and are as follows:

1. The Service Provider must be able to **define the intended purpose(s)** of the services being provided, along with the anticipated impact on health and care outcomes. **(Implemented in the QSF Module "Effectiveness of Service" – Reference ES07)**

   The purposes would for example distinguish between reactive, proactive and preventative service models. We can for example imagine that Reactive (real-time emergency) alarm handling requires that the service and its underlying technology platform is 'always' available when needed. Contrast this with Preventative outbound calling where, depending on the specific service being offered, it may be acceptable for the service or platform to be interrupted for a whole day whilst upgrades are performed.

2. The Service Provider must be able to **define the key operational parameters** which ensure that the service is fit for the intended purpose(s). **(Implemented in the QSF Module "Business Continuity" – Reference BC12)**

   The aim here is to ensure that the Service Provider is considering the key issues that affect 'resilience' when specifying an underlying technology platform or engaging in negotiation with technology suppliers. The parameters are expected to include 'availability of the service on demand', maximum downtime, response times and security requirements.

3. The Service Provider must be able to demonstrate that the intended purposes and key **operational parameters have been shared and agreed upon with buying customers and users. (Implemented in the QSF Module "Effectiveness of Service" – Reference ES08)**

   The aim here is to ensure that customers understand the extent to which they can rely on the care services being provided, and what they are getting for their money. It is expected that Service Level Agreements with customers (commissioners and users) will incorporate the key operational parameters, such as committing to annual 'down times' of less than X hours.

4. The Service Provider must **employ processes that ensure that the service achieves the key operational parameters. (Implemented in the QSF Module "Business Continuity" – Reference BC13)**

   The expectation here is that the Service Provider will design and continue to monitor the performance of the service and underlying technology platform, to make sure it continues to meet the performance that has been promised to customers. The initial and ongoing, monitoring processes will need to demonstrate that people resources, data and enabling technologies are combined in a suitable overall design that meets the agreed performance requirements.

5. The Service Provider must be able to **identify a Design Authority**, who has end-to-end responsibility for ensuring that the combination of enabling technologies and the use of data is fit for use by care staff and users, and hence the intended purpose(s) of the Service. **(Implemented in the QSF Module "Business Continuity" – Reference BC14)**

   It is recognised here that the end-to-end delivery of TEC services can be complex, and the end-to-end understanding of technology platforms, telecommunications, user devices, the associated data processing and skills requirements, is a specialist role. It is proposed that a

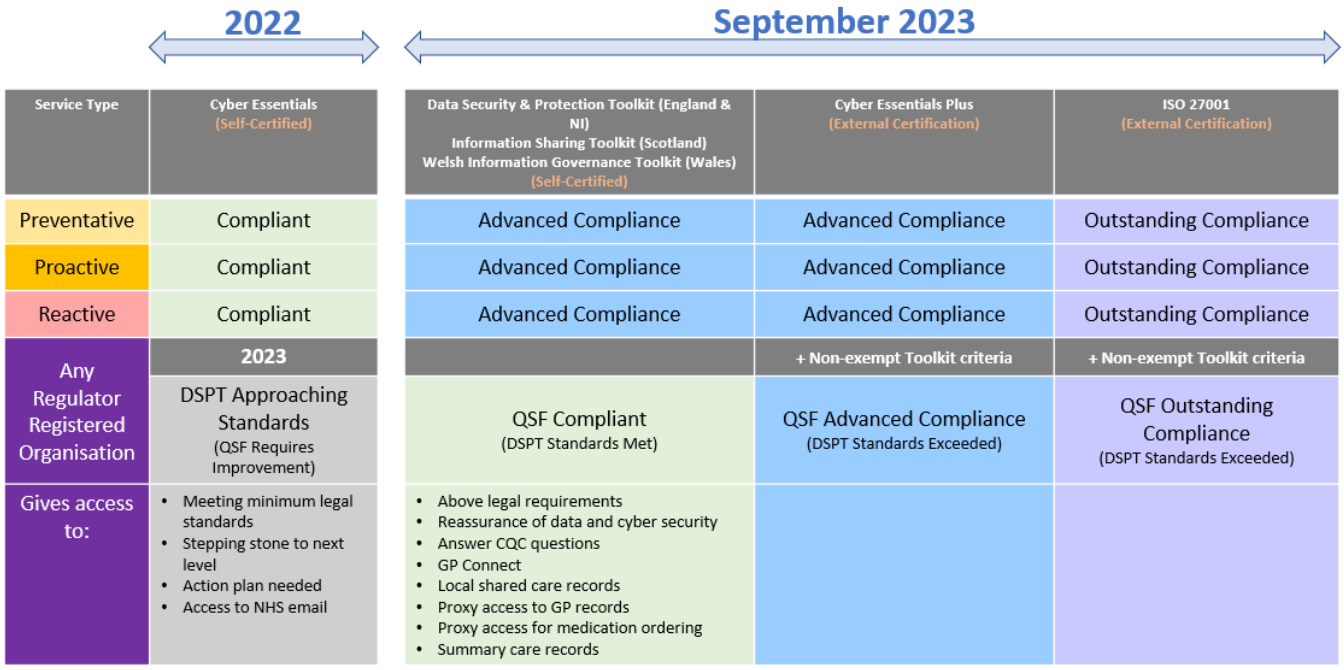
single Design Authority (person or organisation) should be the identifiable owner of these responsibilities.

Timelines: 'Phase Zero' requirements were adopted in the QSF in September 2021 and audits are now being conducted against these requirements.

Phase 1 – Data Protection & Security

This is the first phase that will impact directly on the technical requirements for the services and underlying technology platforms. It establishes the basic requirements for Data Protection and Security.

This phase also introduces the notion of different levels of service 'quality level': Compliant, Advanced Compliance and Outstanding Compliance. The intention is that these quality levels will provide the means of easy comparison of services by commissioning customers and users. However, as already explained, these will be introduced in 2023.



Notes:

a) Consider the example of standards proposed for Data Protection & Security. Here, we can see that 'self-certification' against the Cyber Essential scheme would meet the minimum (Compliant) quality standard. However, higher levels of quality compliance are possible, through independent/external certification (Advanced Compliance) or by certification against ISO27001 (Outstanding Compliance).

b) SIG 008 found no reason to differentiate between service types, given that risks to data loss and disruption apply across the service spectrum.

c) Cyber Essentials has been adopted here by TSA and TEC Quality, given its use within Local Authority procurement. However, the Data Security and Protection Toolkit (DSPT) Toolkit (or other UK equivalent) compliance will be more appropriate and also may be a requirement where services are provided to the NHS and those organisations that are registered with the regulator, CQC, or

Care Inspectorate for example. For the higher levels of quality, there may still be additional requirements within the health toolkits that will need to be met before we can rate the organisation as compliant. More information on these standards can be found below:

a. Data Security and Protection Toolkit (England)
b. Information Sharing Toolkit (Scotland)
c. Welsh Information Governance Toolkit (Wales)

Timelines: It is intended that these 'Phase 1' requirements for 'Compliant services will be adopted into the QSF from **Sept'22** onwards. However, it is anticipated that the quality rating system will be introduced in September 2023.

Phase 2 – Availability of TEC Monitoring Service

Measure 'A': Annualised Availability

This is a key quality measure for any service. It defines the extent to which a service is there and is useable when it is needed. The expectation for potentially life-critical calls is of course that the service and underlying technology are 'always there' and working, although even here there are practical and affordable limits. Availability defines the percentage of time for which the service is operating at its agreed levels of service performance and is fully accessible to users. It is common for the inverse measure, 'downtime', to be quoted (e.g. 48 hours of 'downtime' per year equates to 99.45% availability). The diagram below shows the acceptable levels of availability for a service with 10,000 active end users.

Reactive (Alarm) services are assumed to be operational on a 365-day/24-hour basis.

Proactive and Preventative service availability applies to the contracted service periods (e.g., 0900-1700, Monday-Friday).

Here too, different service tiers, and levels of service 'quality level' apply, and the proposed Quality Measures are as follows:

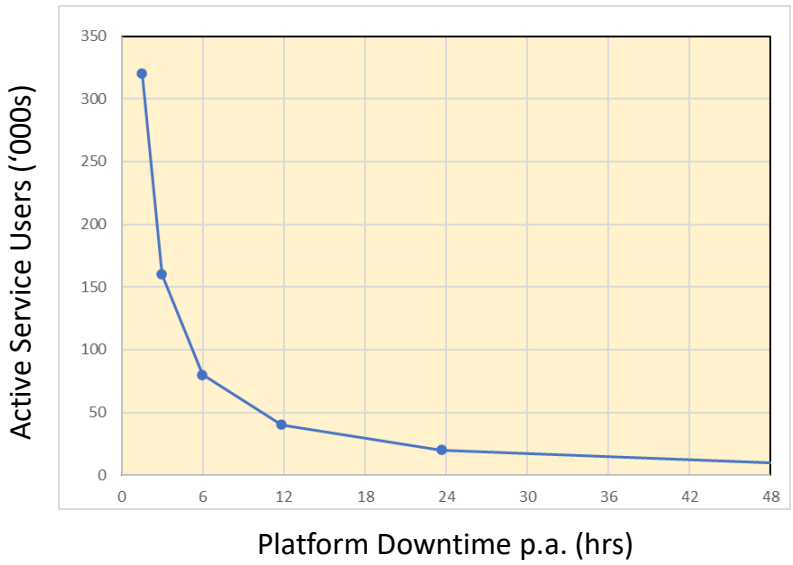
Service Type	Maximum Unavailability (Per annum)				
	96hrs	72hrs	48hrs	8hrs	2hrs
	= 98.91% Availability	= 99.18% Availability	= 99.45% Availability	= 99.91% Availability	= 99.98% Availability
Preventative	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance	Outstanding Compliance
Proactive	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance
Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Minimum acceptable levels of availability for a service with 10,000 active end users.

There are many aspects of a Service and its underlying technology platform that can contribute to downtime, from equipment failure to staff disruption. Different service 'quality levels' can also be defined.

For some service types, such as weekly 'check calls' or health surveys, then a greater service downtime is generally acceptable than for life-critical alarm calls; a technology system failure for say 4hrs could be mitigated by re-scheduling outbound 'check calls', with limited risk.

The scale of the service also has an impact, since larger populations of end users increase the potential for loss of service actions per hour of downtime. In the diagram below, we apply the availability criteria to different service sizes.



Minimum Availability for Size of Reactive Service

(COMPLIANT Quality Level)

Rule of Thumb:

Active Service Users ('000s) x Downtime p.a. (Hrs) must be less than or equal to "480"

Examples:

10 thousand users x 48 hrs downtime <= 480
160 thousand users x 3 hrs downtime <= 480

For REACTIVE TEC Monitoring Services, the main platform components that are involved in alarm handling can be defined, and we are able to describe the guidelines in more detail.

Minimum Availability Targets	Compliant	Advanced Compliance	Outstanding Compliance
Platform Availability is calculated as the aggregate performance of the 4 logical sub-systems are listed below.	≥99.45%	≥99.91%	≥99.98%
1. **Data storage** (including the availability of databases, physical drives, virtual drives, and audio recording storage). Considered unavailable if data storage is inaccessible.			
2. **Compute** (availability of Operating system, applications, microservices, containers, virtual machines, CPU). Considered unavailable if compute provides no useable output.			
3. **Network** (availability of public DNS, Certificates, web interfaces, Internet connectivity, network traffic, VPN connectivity). Considered unavailable if access to the computer and storage layers cannot be achieved.			
4. **Alarm calls/data ingress** (availability of SIP channels, telephone lines, web services, APN-VPN for alarm reception and outbound calls). Considered unavailable if no access to incoming calls/data. And see note f.			

Notes:

a) Aggregate availability is derived here (to a good approximation) by adding downtimes of logical sub-systems, then calculating the inverse platform availability.
b) The frequency of sampling of sub-systems must be no more than 1 minute, with aggregate availability reported per 4hr period.
c) Platform downtime must include any time taken to switch to back-up sub-systems (see also separate measure C).
d) Exemptions will be considered for wide-area (national) failure of communications, cloud services etc.
e) Reporting should cover time periods agreed in Quality Standards Framework and should not be less than the preceding 180 days.
f) For capacity design, line/channel availability should not drop below 80% for more than 10 minutes in a 24-hour period. This should be monitored weekly, and the capacity reviewed and increased if necessary. The determination of line/channel availability will be based on historic call handling data and will consider potential fluctuations in service level and possible increased demand. Where different alarm protocols are used, the measure will apply to individual circuits (i.e. one line, one telephone number) where they are utilised, or aggregated across a bank of two, or more circuits (i.e. multiple lines with one telephone number) where these are used for a single protocol.

Measure B - Maximum Tolerable Single Instance Downtime

There are many aspects of a Service and its underlying technology that can contribute to downtime over the course of a year. These disruptions may arise as a collection of short episodes of downtime. However, a single and extended disruption can pose significant risks to end-users, and it will have a major impact on perceived service quality.

> *The longer a service is down, the more likely that a critical service user will be unable to receive assistance within the "golden hour". Examples of the serious impact of delay include:*
> - *1 hour on the floor after a fall has been cited as equating to 1 extra day in a hospital*
> - *treatment is usually needed within 1 hour after a heart attack to avoid further heart damage or even death*

Therefore, SIG 008 also proposes a quality measure that relates to the maximum tolerable duration of any single disruption, in terms of downtime.

It is important to note that Service downtime will be dependent upon the availability of the primary TEC Monitoring Services platform and also upon the time to re-establish the service using any backup or disaster-recovery facilities.

The quality measures are as follows:

Service Type	Maximum TEC Monitoring Service Downtime				
	12hrs	4hrs	60mins	20mins	10mins
Preventative	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance	Outstanding Compliance
Proactive	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance

Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Maximum Tolerable Single Instance Downtime

Measure 'C' – Recovery Objectives for REACTIVE TEC Monitoring Services

Some suppliers of technology platforms may be more familiar with concepts of 'Recovery Objectives'. Therefore, we have defined the Maximum Tolerable Downtime in terms of such measures for the example of REACTIVE TEC Monitoring Services as follows:

Objective	Compliant	Advanced Compliance	Outstanding Compliance
Recovery Time Objective (RTO) *the time it takes for the TEC Monitoring service to become available again after an interruption.*	Less than or equal 60mins	Less than or equal 20mins	Less than or equal 10mins
Recovery Point Objective (RPO) *the maximum amount of time of data loss when availability is restored (e.g., since the last data backup or replication)*	Less or equal 120mins	Less or equal 40mins	Less or equal 20mins

Notes:

1. For a wide-area communication fault condition, the service should not drop below 80% of the designed telephony capacity for more than 10 minutes, at which point the RTO starts to be measured. Where this measure is breached and where the telephony capacity of the Business Continuity Plan (BCP) solution is not less than that of the main operating site, the BCP solution will have been invoked.

2. RPO is double the RTO targets and reflects that services may be recovered sooner but with the risk of data inaccuracy.

Timelines: It is proposed that all 'Phase 2' requirements will be adopted into the QSF applied from **Sept'23** onwards.

Phase 3 – Outfield Equipment Quality Measures (WORK IN PROGRESS)

The previous application guidelines all apply WITHIN the boundaries of a TEC Monitoring Service Centre.

However, we also need to address the reliability and availability of equipment, networks and applications that connect the Service Centre to its remote users. Here, there are multiple technology solutions to grapple with, along with the challenges posed by analogue to digital migration. Therefore, quality measures for 'Outfield Equipment' are still a work in progress. It is anticipated that the Availability, Data Protection &

Security measures employed for TEC Monitoring Services will carry over in a similar way to Outfield Equipment. Here, we need to note that all the components of end-user equipment, network and intervening applications will need to be addressed.

Additionally, we will need a measure that covers the timely end-to-end performance of the overall system. This may take the form of 'alert transit time' as shown in the diagram below:

Service Type	Maximum time from alert activation by the user to presentation to the operators at the TEC Monitoring Service (Transit Time)			
	>20secs	20secs	10secs	5secs
Critical	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Maximum Alert Transit Time

Until separate standards are agreed upon for 'Outfield Equipment', any Service Design Authority will need to demonstrate that the connectivity of any Outfield Equipment does not significantly degrade the performance of the intended Service below those levels established for the TEC Monitoring Service itself.

Timelines: The Outfield Equipment Special Interest Group is working towards 'Phase 3' requirements that could be adopted into the QSF roadmap and applied from **Sept'24** onwards, and ahead of the final stages of the UK's analogue to digital migration of telecommunications.