PUBLISHED: AUGUST 2020

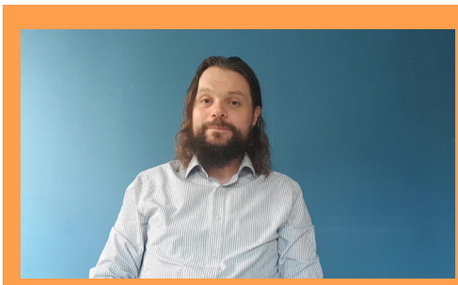
# DIGITAL TELECARE TESTING

Insight Service
DIGITAL TELECARE
Scottish Local Government

Welcome to the August Insight Service where we will look at one of the most fundamental stages for implementing digital telecare; testing, exploring why this is so important and outlining some of the key testing stages.

## WHY TEST?

Testing is an essential part of the process of transitioning to digital telecare, and the reasons for this can be broken down under two key headings: Service Quality and Cyber Security.



Thomas Ozers, Project Manager for Digital Telecare for Scottish Local Government, introduces testing when transitioning to digital telecare.

### Service Quality

For a core service like Telecare, it's essential that you have a high-level of confidence that the system works as expected, that it works reliably and that it offers an acceptable quality of service for users.

Robust testing, and a clear record of the results of that testing, allow you to confidently answer these questions in the affirmative and proceed with user migration. Furthermore not only does it reduce the likelihood of something going wrong with the system, it also provides you with clear evidence that fall due-diligence was undertaken, should any future issues arise.

### Cyber Security

We've spoken at length about the potential for innovation digital telecare offers, particularly in terms of being able to connect a wider range of devices and systems. The flip-side of this is that the greater flexibility and potential of digital signalling protocols also introduces more vulnerabilities into the system which need to be mitigated. But what's the worse that could happen?

**Service disruption** – If an outside party is able to gain access to the ARC solution they could shut down the service. This could be through a deliberately targeted distributed denial of service (DDOS) or ransomware attack by a criminal gang, but equally it could be the unintentional consequences of a bored teenager seeing if they can hack in without really understanding what the service is.

**Data loss** – ARC's by their very nature hold a significant amount of sensitive personal information, and so it's essential to ensure that this information is secure and cannot be accessed, either mistakenly or maliciously, by anyone without a valid reason for doing so. Any data breach could cause significant distress for service users, erode their confidence in the service, and lead to significant fines.

**Misuse of equipment** – There is a well-publicised case from England of a partnership receiving a phone bill for thousands of pounds after a service user's grandson removed the sim card from their GSM alarm and used it to play Pokémon.

As scary as all of this should sound, these are risks which can be mitigated, and we'll now explore three key testing stages which do just that.

## THREE KEY TESTING STAGES

### Penetration Testing

Penetration testing, also known as 'ethical hacking' or 'pen testing' for short, involves a specialist company testing the cyber security of your solution by simulating a variety of scenarios such as a cyber-attack or accidental misuse. Through this they identify possible vulnerabilities in your system allowing measures to be taken to address them.

By assessing that your system is secure pen testing provides a level of assurance against:

Theft of data;
Accidental data breaches;
Misuse of sim cards in GSM devices;
Some forms of denial of service attacks.[1]

Our Guide to Penetration Testing is contained within the document library of the Digital Telecare Playbook and provides an in-depth overview.

The Digital Office's Chief Information Security Officer, Andy Grayland, has secured a company to undertake 128 days of pen testing on behalf of Partnerships. These hours will be allotted on a first-come-first-served-basis, but it is anticipated that each council test will take approximately 4 days. For more information email digitaltelecare@digitaloffice.scot.

### Internal Acceptance Testing (IAT)

Internal Acceptance Testing is the process by which partnership staff check that the new digital telecare system works, that it is reliable and that it offers a better level of service, in terms of quality and reliability, than existing analogue systems. This is done by issuing alarm devices, and in some instances peripherals, to group of staff volunteers who take them home and make test calls with them.

IAT helps mitigate risks to service users by ensuring that everything is working properly before it is rolled out to live users.

The Digital Telecare Playbook includes a number of templates to support IAT and the Digital Telecare team can provide support for Partnerships planning IAT.

### User Acceptance Testing (UAT)

The final stage of testing, UAT sees the digital telecare solution rolled out to a carefully selected sample group of real users. This is normally done in two stages, first with 'low-risk users' and then once that has been successfully completed, with 'high-risk users'.

It is ultimately for Partnerships to define exactly who qualifies as a low-risk or high-risk user, but the Digital Telecare team suggest the following definition as a starting point:

- **Low Risk User** - this is a user who is only supplied with a pendant, rather than a more complex telecare package, and for whom a short period of unavailability of the telecare service would be tolerable.
- **High Risk User** - this is a user who has a complex telecare package, and/or a user for whom a short period of unavailability of the telecare service would not be tolerable.

UAT focuses on the end-user experience, ensuring that they are able to use the equipment is easy for them to use, works as expected and offers a good standard of service.

Our Guide to Planning Internal and User Acceptance Testing can be accessed via the document library on the Digital Telecare Playbook and provides a comprehensive overview of UAT including the different test criteria you should include.

We're currently working on communication templates to support Partnerships to recruit users for testing, and again the Digital Telecare team can provide additional support to Partnerships preparing for, and undertaking, user testing.

## INTERVIEW WITH HAMISH JOHNSTON

To provide a bit more insight into the testing process we caught up with **Hamish Johnston, Project Manager with Moray Health and Social Care Partnership**. Hamish has a wealth of experience of testing in the public sector, and has been involved in a huge variety of projects from custody systems for the Metropolitan Police through to data sharing in Grampian. Most recently Hamish has been leading on Moray's Test of Change which is testing new GSM equipment created by Chiptech.

### Why do you think testing is important and what are the key benefits?

Testing should ensure that the product has no errors for the user (management, IT and front end) when a system goes 'Live'. Testing does not include functionality (whether the system delivers the functionality required by the User Requirement (UR)): this is the responsibility of the Project Team to examine the delivered functionality against the user requirement prior to testing. Testing also should cover:

- Whether the system is stable;
- Load, performance and stress testing;
- Security.

Simply, testing will deliver the answer to the question, "does it do what it says on the tin?" – is the system reliable; but I emphasise, it is the supplier's tin not the customer's tin. Obviously if testing shows major gaps in the UR then testing will stop but that is the decision for the Project Manager not the Test Manager.

### What are the key points to consider when implementing testing?

Once testing starts the main things for a manager to watch are errors and timescales – the judgement of the seriousness of any errors and what fixes are required; this will impact on timescales.

Also, as testing progresses, are there sufficient testers (or too many); this will also impact on timescales. A manager must constantly review the progress of testing against the Test Plan – is the testing delivering against the Plan – does the Plan need adjusting? The manager must make a decision, if necessary, as to whether testing should stop or be suspended because the Error Count is too high. Finally, the manager must decide whether the results of testing meet the Exit Criteria.

**What are the key stages to consider when planning testing?**

1. What is the purpose of the test?
2. What is to be tested?
3. How is the testing to be carried out?
4. Service Level Agreements and Data
5. Scope
6. Test Management
7. Timescales
8. Pre-Requisites
9. Hardware
10. Prior Testing
11. Training
12. Approach
13. Test data
14. Communications
15. Roles
16. Conducting the Tests
17. Process
18. Errors and Fixes
19. Supplier Support
20. Escalation Process

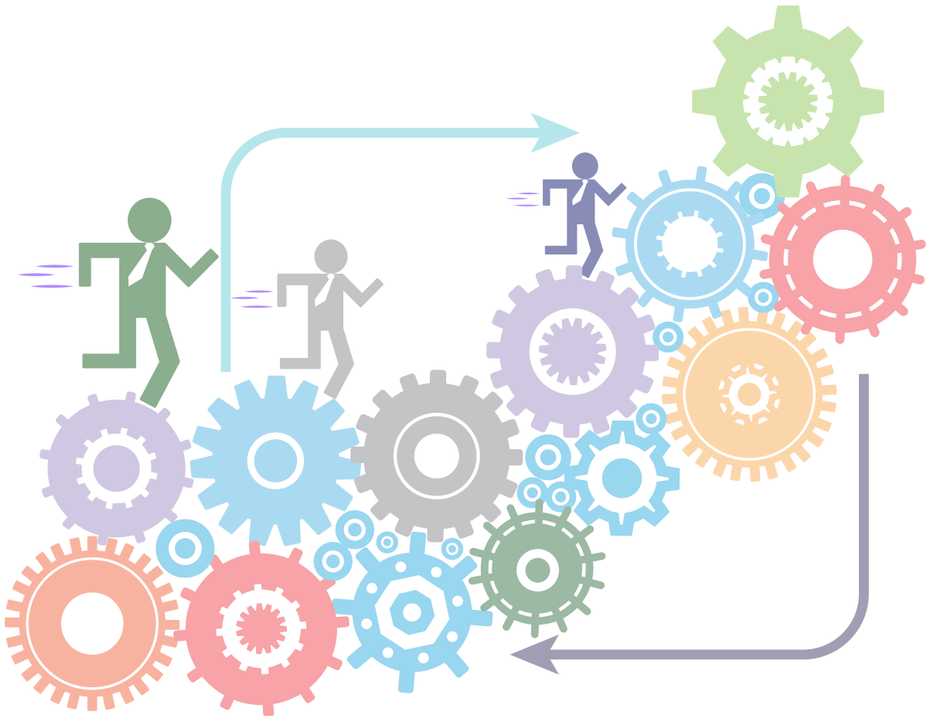
### What are the pitfalls Partnerships might not be aware of?

The main error that occurs is that management will ignore the error count in order to implement a system; this is not a decision for the Test Manager but too often means that what is delivered is not fit-for-purpose.

### Any final thoughts that you would like to share?

My principle for testing is Test, Test and Test again. Do not sign off testing until and unless you are completely satisfied that the Exit Criteria has been met. Be willing to stop or suspend testing if the Error Count is too high. Do not be pressured to just, "get the thing in."

If you have any questions relating to this Insight Service or the wider Digital Telecare work, please get in touch with the Digital Telecare for Scottish Local Government team.



1 Note, DDoS cannot be mitigated against through pen-testing. Factors to protect against DDoS include having a disaster recovery site and having multiple Device Management Platforms (DMP) or a DDoS resilient DMP