Inspections and Audit Trends

Rumors

IT Inspection, preparations

- Arranged meetings
- Understood that IT would be an important element
- Established an PV/IT Inspection Preparation Team
- Developed our own IT check-list and identified relevant systems

Important factors

- Inspector
- **Days**
- **Areas**
- **SMEs/ Staff**
- **Facilities/ Practical Issues**

Pre-notification activities Early 2018

- Got a new team member; previous Lead Inspector
- Meeting early January in order to get intelligence from the former DKMA Inspector
- Very clear message:
- Calm down, - DKMA does not have the resources until Q2, - at the earliest

T

- So we relaxed!!!!!
- The Inspection Notification came 17th January 2018

LEO

IT Inspection, preparations

IT Group

- Did not get any initial requests!!!!!
- Revisited the PSMF in order to ensure that they had identified all relevant computerized systems

Approaching Inspection

05.03 Afternoon	Contracts continued	GCP activities	IT systems
	Quality system/management • Introduction to the quality system • Introduction to training • Review of training documentation • Review of other staff documentation **Follow up on status on CAPA's from previous inspections**		

Approaching Inspection

Training (summary) by Mark Twain

- If you tell the truth, you don't have to remember anything.
- It is better to keep your mouth closed and let people think you are a fool than to open it and remove all doubt.

Approaching Inspection

Last Minute Preparations

- Arranging the Inspection Facilities
- Done 2 March 2018 (Friday……)
- Staff had to leave LEO early, - due to snowstorm
- At 1.40 pm an e-mail was sent from the IT Inspector, who asked for “Complete URS” for 6 Computerised Systems
- We said: Yes we can!!!!, and did it!

Inspection conduct

Practicalities: Inspection in I-32

Inspection conduct

Inspection conduct

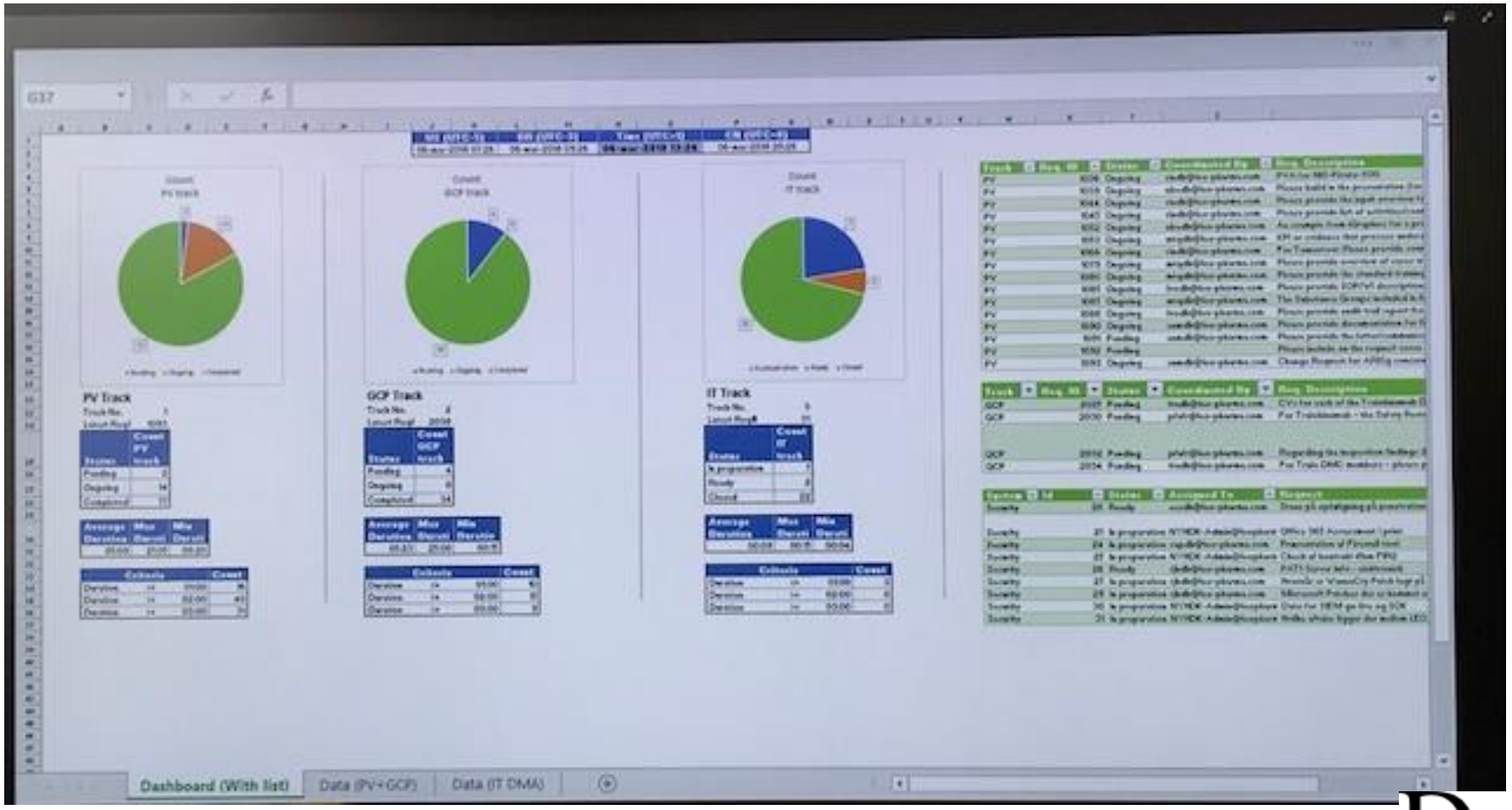
Boiler Room

Ongoing Inspection

Boiler Room

Inspection conduct

Boiler room Request Tracking Screen



Inspection conduct
Outcome

- The inspectors generated a record high number of requests during the inspection
- Inspectors arrived at 9 am each morning and stayed until 18:30 – 19:00 with a few exceptions; the IT Inspector continued the activities in the IT track until 21:06 and left 21.30 on 8th March
- A total of 840 requests were received and replied during the inspection, status after each day was that 90 – 95 % had been closed
  - 221 requests in the PV track
  - 107 requests in the GCP track
  - 502 requests in the IT track

Inspection Conduct

IT track

- Worked from an excel spreadsheet
- Identified 5 Systems and 2 interfaces for Inspection (actually 7 systems, but one was skipped, and one was out of scope)
- Used > 60 generic questions for each system
- Areas of interest were Validation, Data Integrity, - Security/Disaster Recovery

IT Track

Examples of areas inspected

MHRA GCP INSPECTIONS METRICS REPORT

PERIOD: 1st April 2016 to 31st March 2017; issued 11 May 2018

Medicines & Healthcare products Regulatory Agency

MHRA
Regulating Medicines and Medical Devices

MHRA Recent Inspection Metrics

Critical Finding 5

A critical finding was given to a commercial sponsor for Data Management due to processes relating in particular to data generated through electronic patient reported outcome (ePRO) devices. The following issues were identified:

- There was incorrect data in the eDiary that could not be changed, but was used for the analysis. Data Change Forms (DCFs) had been submitted by Investigators to change entries for data entered by both site staff and subjects that which had been identified as incorrect. These requests were denied as it was explained that changes to the data could not be made and the investigator would need to document the response in the source.

MHRA Recent Inspection Metrics

Critical Finding cont

- The eDiary devices used by subjects did not have an audit trail to verify when entries were being made and by whom. Whilst the data provided to the investigators contained a form “save time” this was not reflective of when data was actually entered and there was no way to verify who entered the data as user name and login were not captured in the audit trail.
- There was lack of information provided in DCFs regarding what the query was. It was explained that data could only be changed via a DCF. However, examples were seen where the DCF lacked detail and information and referenced a helpdesk ticket number. These were not available in the eTMF nor were they provided to investigators to reconstruct changes to source data.

MHRA Recent Inspection Metrics

Critical Finding cont

- It was explained that data from different devices could be merged (e.g. for replacement devices) and an auto-merge code generated. However, as there was no list of device IDs demonstrating who had been assigned the device (in the TMF), it was not possible to reconstruct which devices had been merged.

- The portal used to manage DCFs did not have an audit trail, so if changes were made to a request after it was submitted by the investigator these could not be identified.

MHRA Recent Inspection Metrics

Critical Finding Cont.

- There was no overall list or tracking of users to the system and their access rights when they were granted and revoked to verify who was managing and making data changes in the portal.

- There was a loss of PI control of data between database lock and pdfs being sent to the site. The pdfs returned were also only the final version of the data and did not contain all meta data.