Data Integrity – Issues:
Understanding and Resolution

The considered views of a UK GMDP Inspector

Rachel Carmichael, GMDP Inspector, 8th Sep 2014

Data Integrity – Issues:
Understanding and Resolution

Session 1

- Introduction to the MHRA, the Inspectorate and inspections
- Overview of data integrity & self-inspection programs

Session 2

- Requirements for Data Integrity - Chapter 4 (Documentation)
- ....as well as a little bit of Chapter 1 and Chapter 6

Session 3

- Requirements for Annex 11 - Computerised Systems
- Examples of typical deficiencies

Data integrity from IEEE*

- The degree to which a collection of data is complete, consistent, and accurate

*Institute of Electrical and Electronics Engineers

Data integrity from Wikipedia!

Data integrity refers to maintaining and assuring the accuracy and consistency of data over the entire data life-cycle:

- ensure data is recorded exactly as intended

- upon later retrieval, ensure the data is the same as it was when it was originally recorded

Data Integrity - issues

Conscious Competence Learning matrix
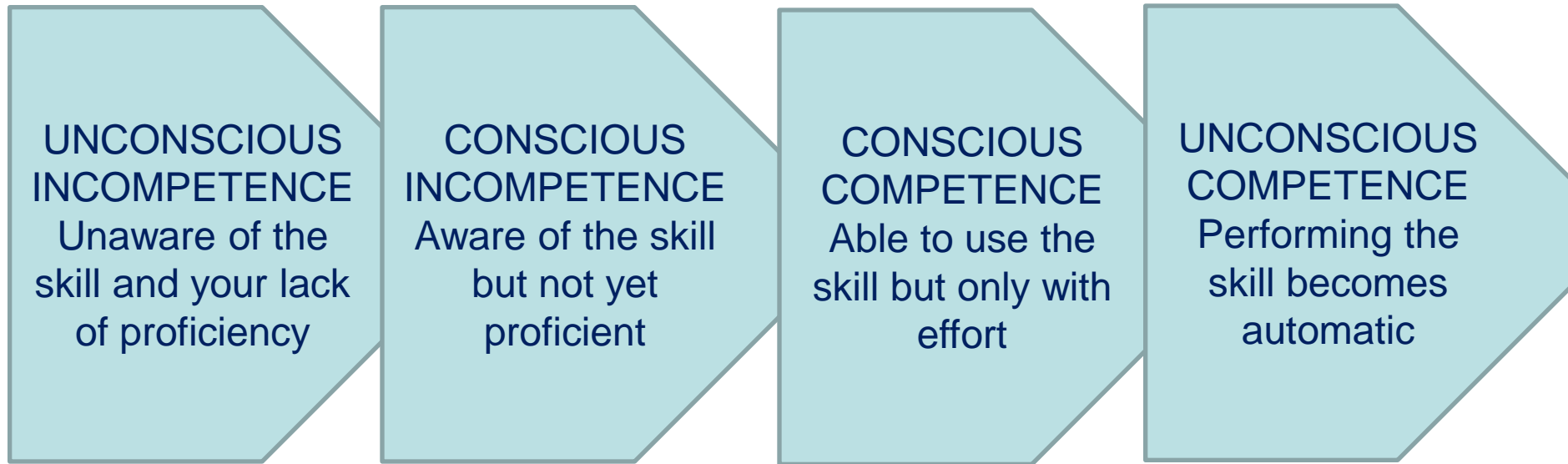
MHRA

| UNCONSCIOUS INCOMPETENCE Unaware of the skill and your lack of proficiency | CONSCIOUS INCOMPETENCE Aware of the skill but not yet proficient | CONSCIOUS COMPETENCE Able to use the skill but only with effort | UNCONSCIOUS COMPETENCE Performing the skill becomes automatic |

Corporate Consciousness – Data Integrity

UNCONSCIOUS INCOMPETENCE
Do not know about the issue and unaware of the gap

CONSCIOUS INCOMPETENCE
Aware of the gap but not yet able to deal with it

CONSCIOUS COMPETENCE
Getting a handle on the problem but only with effort

UNCONSCIOUS COMPETENCE
Good practice becomes automatic

Corporate Consciousness – Data Integrity

UNCONSCIOUS INCOMPETENCE
Do not know about the issue and unaware of the gap

Company not aware of the existence or relevance of the issue

Company not aware that they have a particular deficiency in the area concerned

Company might deny the relevance or usefulness of addressing the issue

Company must become conscious of their incompetence before development of a solution can begin

Management and if necessary Regulators must move the Organisation into the 'conscious competence' stage, by demonstrating the gap and identifying the benefit that addressing it will bring to the Organisation

Corporate Consciousness – Data Integrity

MHRA

CONSCIOUS INCOMPETENCE
Aware of the gap but not yet able to deal with it

Company aware of the existence and relevance of the issue

Company is therefore also aware of their deficiency in this area

Company need to recognise that by addressing the issue their Compliance will improve

(and therefore the long term sustainability of the Organisation)

Ideally the Company has a measure of the extent of their deficiency in this area and a measure of where they need to be (Gap assessment / CAPA)

Company makes a commitment to address the issue and to move to the 'conscious competence' stage

Corporate Consciousness – Data Integrity

CONSCIOUS
COMPETENCE
Getting a handle
on the problem but
only with effort

Company implements the structure, processes and systems to ensure good data integrity is the minimum standard

Company will need to remain alert – concentration will be required, continued Self Inspection

Staff can perform the requirements without assistance (through Procedures and Training)

Staff may not reliably perform the skill unless thinking about it - the skill is not yet 'second nature' or 'automatic'

Staff shall continue to operate in line with the new requirements and in time become 'unconsciously competent'

Corporate Consciousness – Data Integrity

UNCONSCIOUS COMPETENCE
Good practice becomes automatic

Good data practices become so ingrained that it enters the unconscious parts of the Organisation - it becomes 'second nature' like walking, breathing

Staff might now be able to teach others in the skill concerned, although after some time of being unconsciously competent the person might actually have difficulty in explaining exactly how they do it - the skill has become largely instinctual

This gives rise to the need for long-standing unconscious competence to be checked periodically against standards – Corporate Audits/External Auditor

Corporate Consciousness – Data Integrity

UNCONSCIOUS INCOMPETENCE
Do not know about the issue and unaware of the gap

CONSCIOUS INCOMPETENCE
Aware of the gap but not yet able to deal with it

CONSCIOUS COMPETENCE
Getting a handle on the problem but only with effort

UNCONSCIOUS COMPETENCE
Good practice becomes automatic

Session 1

Introduction to the MHRA, the Inspectorate and inspections
Overview of data integrity & self-inspection programs

The Medicines and Healthcare Products Regulatory Agency

The Agency - Overview

Executive Agency

Government Trading Fund and an Executive Agency of the Department of Health established on 1 April 2003

Size

Around 1270 staff, with a total budget of approximately £150 million

Location

Head office at 151 Buckingham Palace Road, London

NIBSC based at South Mimms, Hertfordshire

A regional office in York

British Pharmacopoeia and MHRA laboratories based at the laboratories of the Laboratory of the Government Chemist in Teddington

MHRA – Our Vision

We **protect and improve** the health of millions of people every day through the effective regulation of medicines and medical devices, underpinned by science and research

Centres and Divisions

Medicines and Healthcare Products Regulatory Agency

- Policy
- Communications
- CPRD Centre
- Vigilance & Risk Management of Medicines
- Devices
- Operations & Finance
- MHRA Centre
- Human Resources
- Licensing
- Inspection, Enforcement & Standards
- NIBSC Centre
- Information Management
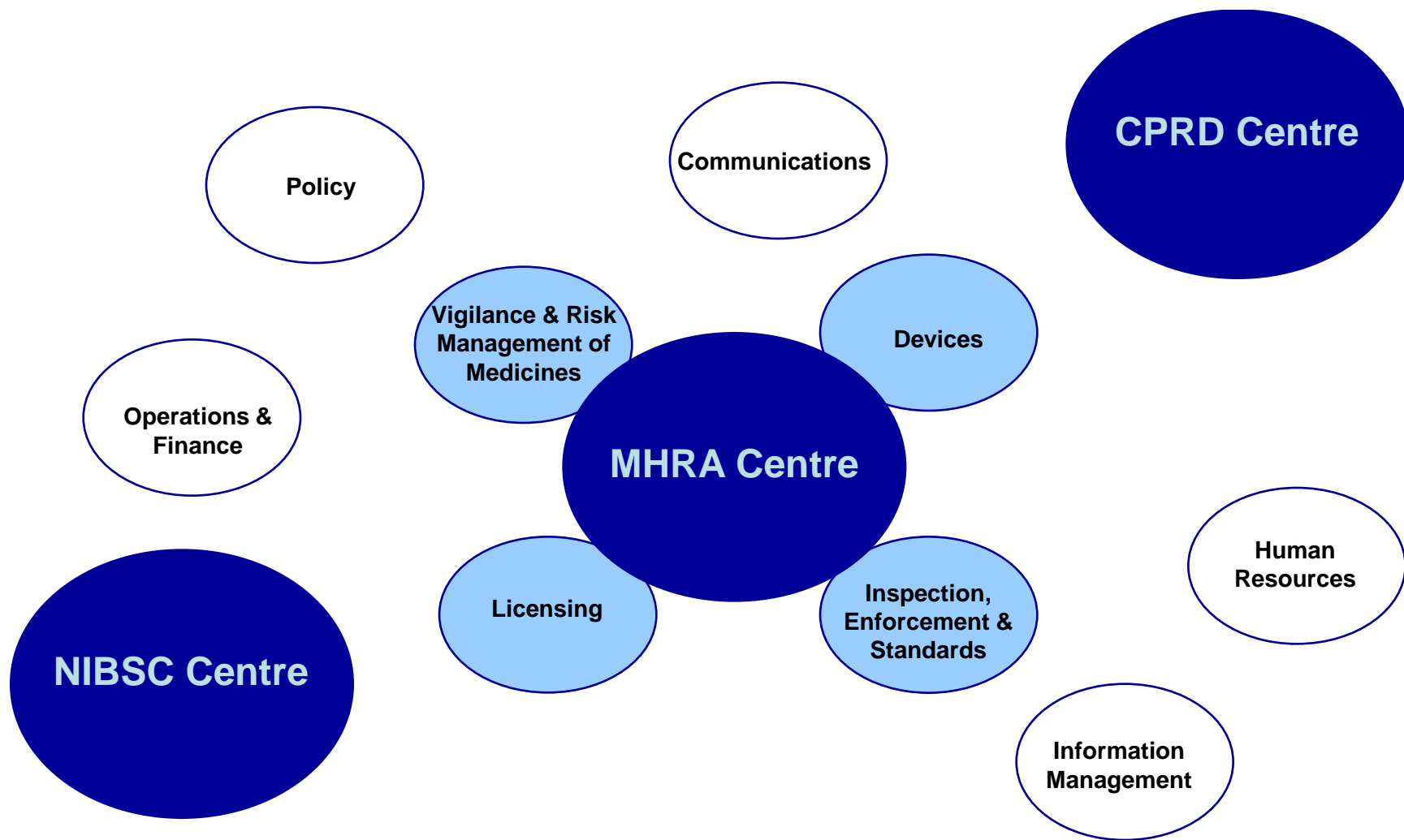
The Agency - Organisation

- **MHRA**
  - Regulates medicines and medical devices, ensuring that they work, and are acceptably safe; focusing on the core activities of product licensing, inspection and enforcement, and pharmacovigilance
  - Designated UK Competent Authority for Blood safety and quality

- **Clinical Practice Research Datalink (CPRD)**
  - Gives access to an unparalleled resource for conducting observational research and improving the efficiency of interventional research, across all areas of health, medicines and devices

- **National Institute for Biological Standards and Control (NIBSC)**
  - World leaders in assuring the quality of biological medicines through product testing, developing standards and reference materials and carrying out applied research

- **Corporate divisions**
  - Communications, human resources, operations and finance, information management, policy

MHRA: Background - Governance & Accountability

- MHRA acts for the Secretary of State for Health, but at 'Arm's Length'

- Staff are Civil Servants

- Agency Board (Chairman and non-executive directors) accountable to Health Ministers

- Chief executive accountable to Parliament through Ministers

MHRA: Background

Statutory role under the Medicines Act 1968 (now Human Medicines Regulations 2012), and other EU legislation for the regulation of:

- Medicines
- Clinical trials of medicines
- Advanced therapies (gene, stem cell, tissue-engineered)
- Medical devices
- Blood safety and quality
- Herbal medicines

Is funded by fees charged to industry, and under a Service Level Agreement with the Department of Health

Supports scientific committees on the safety of medicines (CHM) and devices (CSD) which advise Ministers

The European regulatory network

- 28 member states in European Union (over 500 million people)
- Legislation set up at European Union level

- Medicines: authorisation at national, EU or in a number of countries
- European Medicines Agency (EMA)
- Heads of Medicines Agencies network (uniting 44 regulators)

European Interfaces (GMP)

European Medicines Agency
>GMP GDP Inspectors Working Group
>>Compliance Group (manages JAP)
>
>Inspections
>Roadmap to 2015

European Commission

Heads of Medicines Agencies
>Joint Audit Programme JAP - to demonstrate equivalent GMP Inspectorates
>Benchmarking European Medicines Agencies (BEMA)
>Strategy paper (2011-2015) Risk based re-deployment of inspections

Council of Europe

European Directorate for the Quality of Medicines and Healthcare (EDQM)

Worldwide Interfaces (GMP)

The Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co- operation Scheme (jointly referred to as PIC/S)

Meetings/training, Expert circles, Joint Reassessment Programme

World Health Organisation

Pre-qualification programme inspections, Global Fund/Gates – China, Technical guidance and documents

International Conference Harmonisation (ICH)

Mutual Recognition Agreements

Conformity Assessment and Acceptance of Industrial Products (ACCA)

Bilaterals

Bilateral links

Russia
under negotiation/not taken
forward at the moment

India
under negotiation

Kosovo

China

Canada

Hong Kong
under negotiation

USA

Japan

Taiwan (ROC)

Singapore

Brazil

Ghana

Australia

New Zealand

Confidentiality agreement

Memorandum of Understanding

24
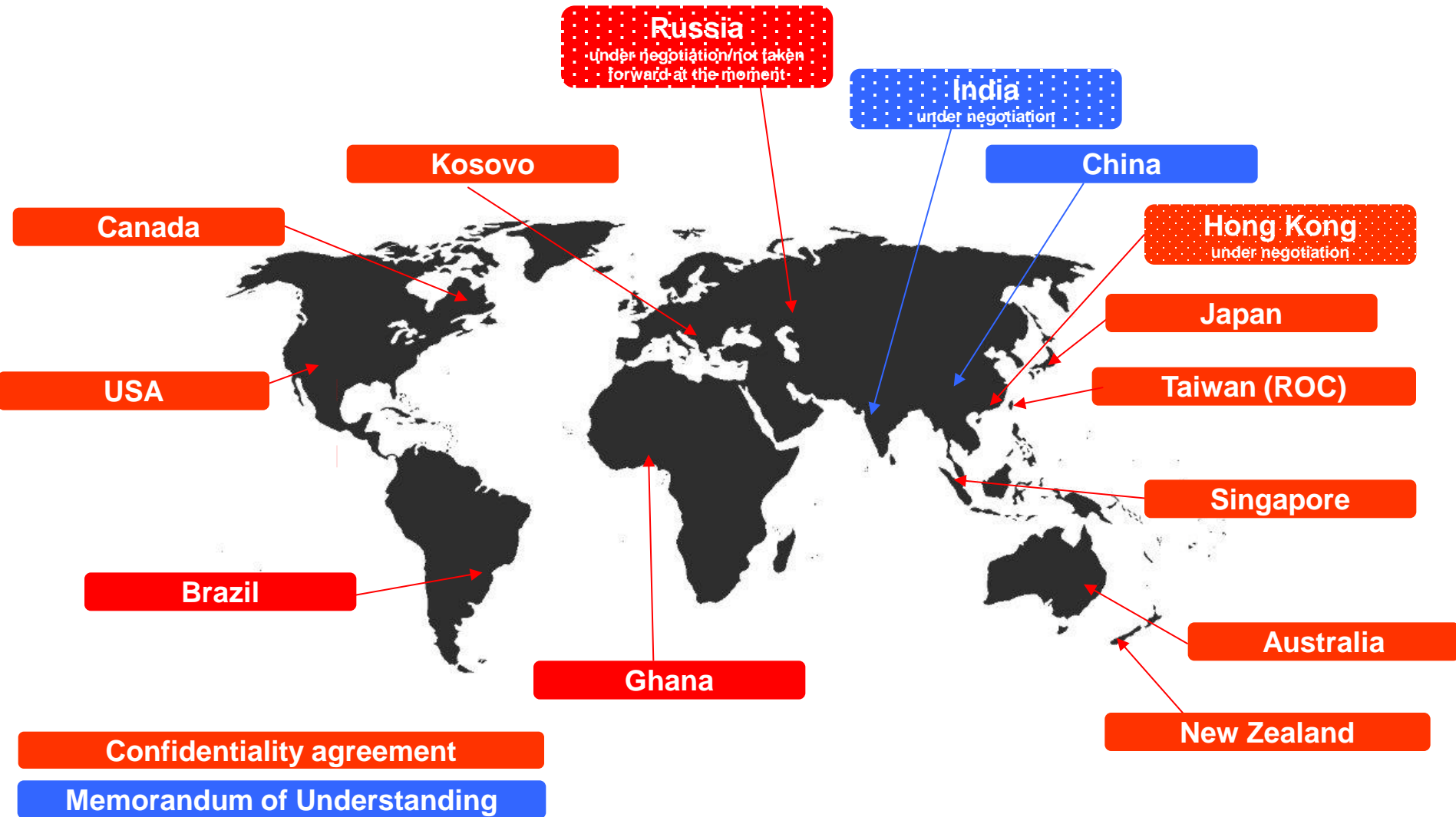
The Importance Of India to UK

- Produces 10% of world's medicines

- 70% of UK medicines are generic

- 23% of UK Product Licences name an Indian manufacturer

- 38% of UK Product Licences name an Indian API source

Active Substance supply sites

42 source countries with 1562 manufacturers:

The Inspectorate

Inspection, Enforcement & Standards Division

MHRA

```
                    ┌─────────────────────────┐
                    │        Director          │
                    │    Mr Gerald Heddell      │
                    └─────────────────────────┘
                              │
                    ┌─────────────────────────┐
                    │  Personal Assistant:     │
                    │  Ms Janet Rickards        │
                    └─────────────────────────┘
```

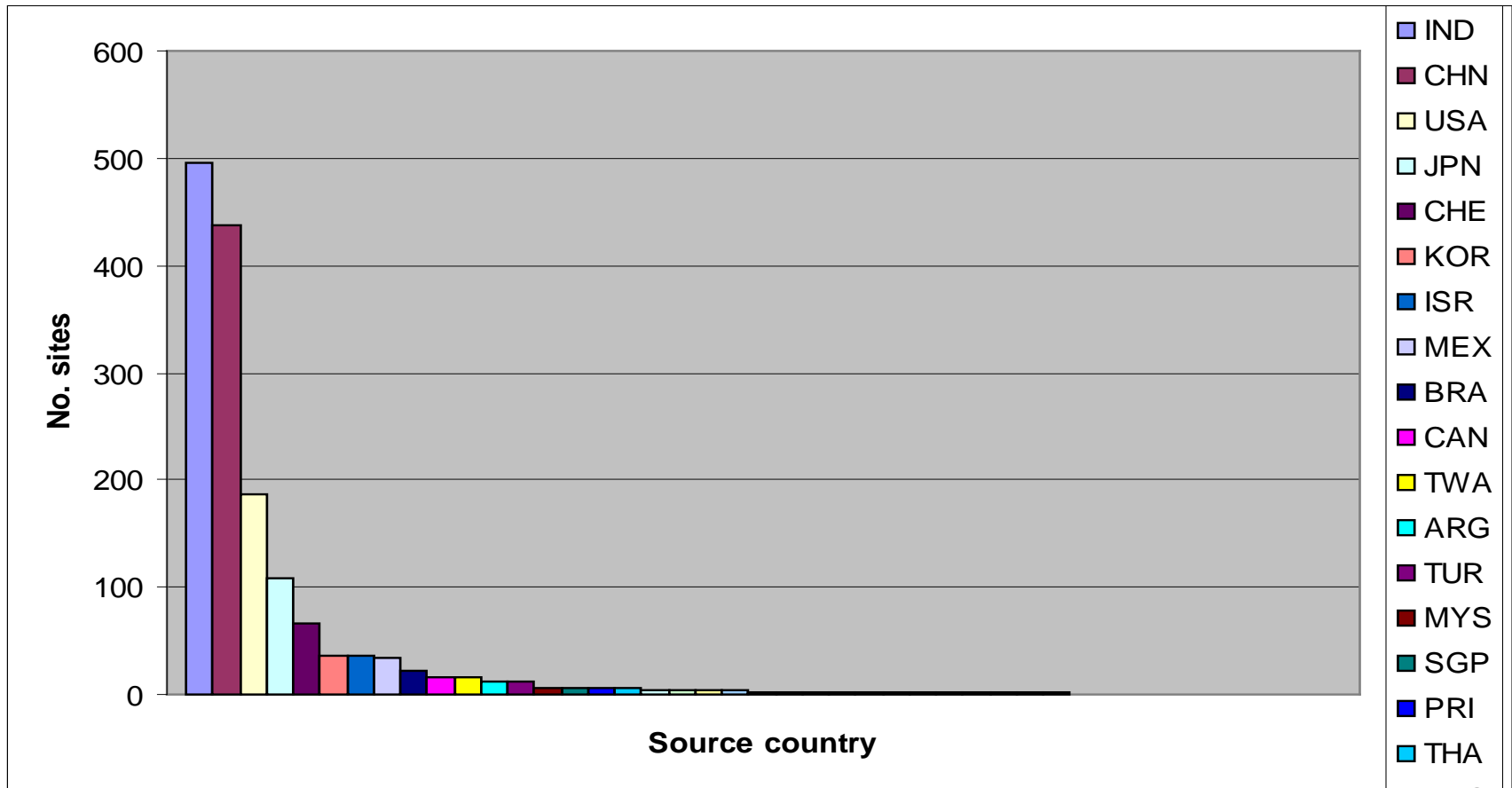| Group Manager Inspectorate **Mr Mark Birse**	Group Manager Enforcement **Mr Alastair Jeffrey**	Group Manager BP & Laboratory Services and BP Secretary & Scientific Director **Dr Samantha Atkinson**	Unit Manager Regulatory **Mrs Bernadette Sinclair-Jenkins**	MHRA Quality Standards Manager **Mr John Taylor**	Unit Manager Business Unit **Mr Joe Kyne**
Inspectorate	Enforcement	BP and Laboratories and Divisional Quality Standards Function	Borderline IAG & Regulatory Advice Pharmaceutical Assessment	Agency Quality Systems Manager	Admin Team Data Processing QMS Computer Support Team

Inspectorate

Group Manager, Inspectorate
Mr Mark Birse
Tel: 020 3080 6036

Business Support Executive
Beverley Malin-Smith
020 3080 7029

Unit Manager
Inspectorate Operations
GMP/GPvP
Richard Andrews
020 3080 6032

Unit Manager
Inspectorate Operations
GCP/GDP/GLP
Andy Gray
020 3080 7510

Unit Manager
Inspectorate Strategy
Ian Rees
020 3080 6058

Unit Manager
Inspectorate Risk, Control and
Governance
Vacancy

GMP Inspectorate

GPvP Inspectorate

GCP Inspectorate

GDP Inspectorate

GLP Inspectorate

Expert Inspectors

Inspectorate Training Manager

Inspection Services Executives

Inspectorate Risk Manager

Inspection, Enforcement & Standards Division
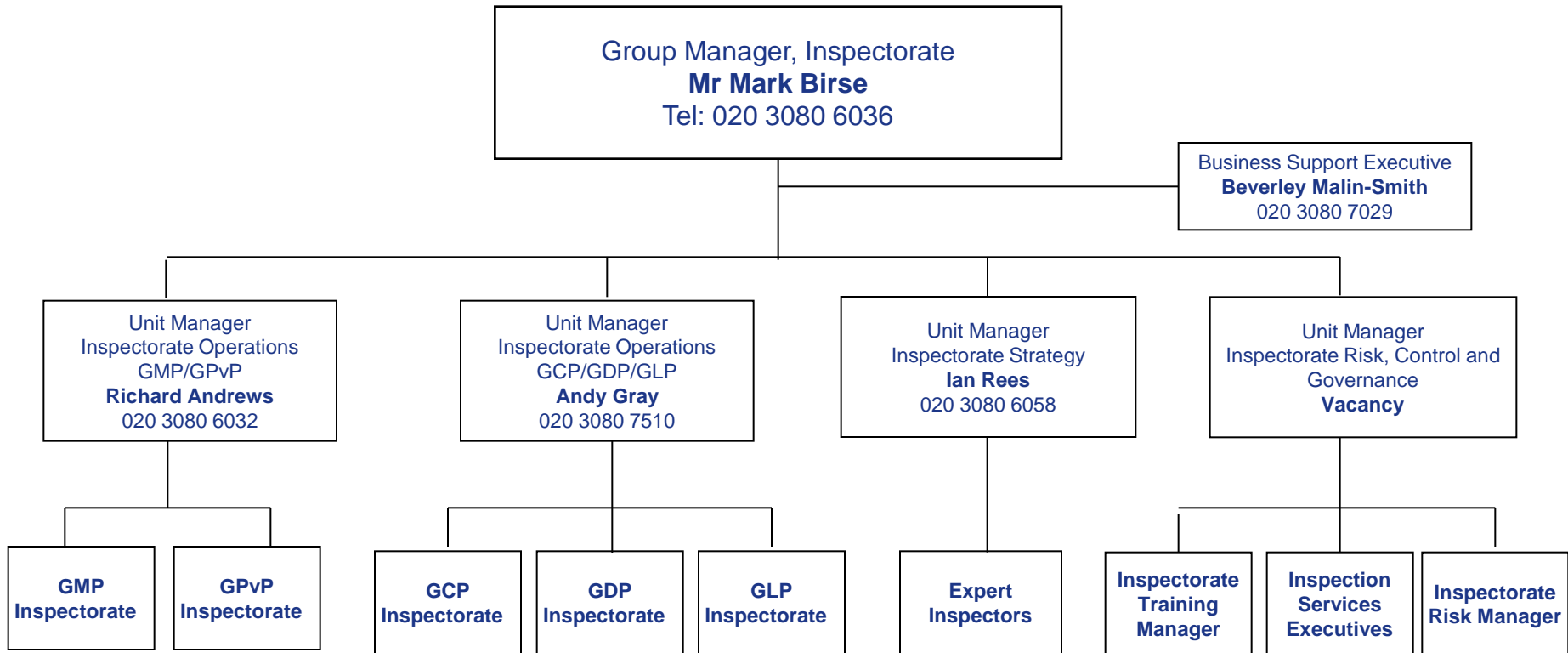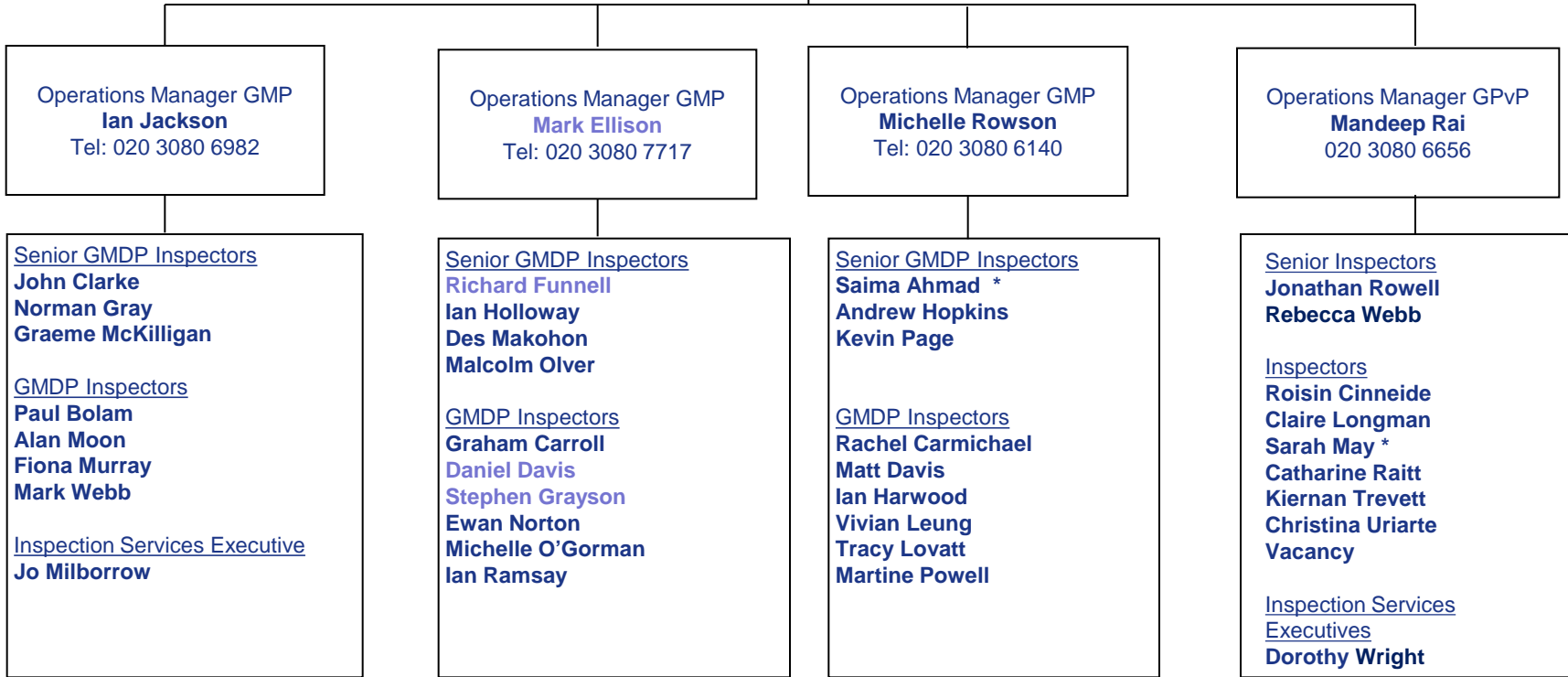
Inspectorate

maternity leave
General contact:
inspectionplanning@mhra.gsi.gov.uk
gmpinspectorate@mhra.gsi.gov.uk

Unit Manager, Inspectorate (GMP/GPvP)
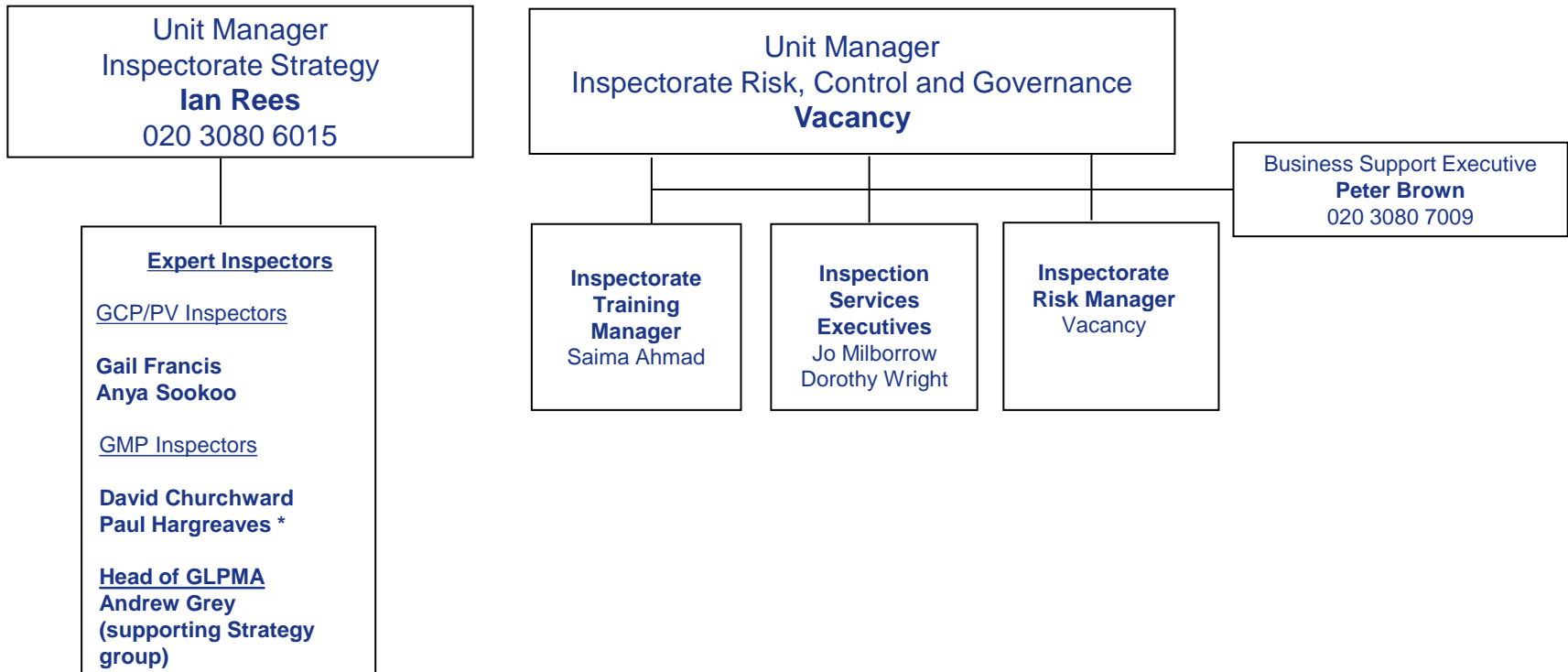**Richard Andrews**
Tel: 0203 080 6032

Operations Manager GMP
Ian Jackson
Tel: 020 3080 6982

Operations Manager GMP
Mark Ellison
Tel: 020 3080 7717

Operations Manager GMP
Michelle Rowson
Tel: 020 3080 6140

Operations Manager GPvP
Mandeep Rai
020 3080 6656

Senior GMDP Inspectors
John Clarke
Norman Gray
Graeme McKilligan

GMDP Inspectors
Paul Bolam
Alan Moon
Fiona Murray
Mark Webb

Inspection Services Executive
Jo Milborrow

Senior GMDP Inspectors
Richard Funnell
Ian Holloway
Des Makohon
Malcolm Olver

GMDP Inspectors
Graham Carroll
Daniel Davis
Stephen Grayson
Ewan Norton
Michelle O'Gorman
Ian Ramsay

Senior GMDP Inspectors
Saima Ahmad *
Andrew Hopkins
Kevin Page

GMDP Inspectors
Rachel Carmichael
Matt Davis
Ian Harwood
Vivian Leung
Tracy Lovatt
Martine Powell

Senior Inspectors
Jonathan Rowell
Rebecca Webb

Inspectors
Roisin Cinneide
Claire Longman
Sarah May *
Catharine Raitt
Kiernan Trevett
Christina Uriarte
Vacancy

Inspection Services
Executives
Dorothy Wright

Inspectorate

MHRA

Acting Unit Manager, Inspectorate (GCP, GDP/GLP)
Andy Gray
Tel: 020 3080 7510

Operations Manager GCP
Vincent Yeung
020 3080 6218

Operations Manager
Stakeholder Lead
Paula Walker *
020 3080 6894

* Maternity Leave

Operations Manager GLP
Christine Gray
01904 406088

Operations Manager GDP
Peter Coombs
Tel: 020 3080 6055

Operations Manager GDP
Philip Neal
020 3080 6108

Senior Inspectors
Andy Fisher
Jennifer Martin
Kathleen Meely

Inspectors
Sue Buchanan
Mandy Budwal-Jagait
Agathe Guillot
Amy Mollallegn
Balall Naeem
Jason Walkelin-Smith
Emma Whale

GLP Team Members

Senior Inspectors
Lesley Graham

Inspectors
Peter Connaughton
Rachel Sayer
Stephen Vinter
Jason Wakelin-Smith

Senior GDP Inspectors
Tony Orme

GDP Inspectors
Sara Berry
Cheryl Blake
Gaynor Brummitt
Jackie Gearey
Clement Lagalice
Jacqueline Masayi
Shahbaz Sarwar

Senior GDP Inspectors
Steve Todd

GDP Inspectors
Madeleine Ault
Alan Bentley
Peter Blundell
Claire Glenister
Katie Journet
Terence Madigan

MHRA

Inspectorate

Unit Manager
Inspectorate Strategy
Ian Rees
020 3080 6015

Unit Manager
Inspectorate Risk, Control and Governance
Vacancy

Business Support Executive
Peter Brown
020 3080 7009

Expert Inspectors

GCP/PV Inspectors

**Gail Francis
Anya Sookoo**

GMP Inspectors

**David Churchward
Paul Hargreaves ***

**Head of GLPMA
Andrew Grey
(supporting Strategy
group)**

**Inspectorate
Training
Manager**
Saima Ahmad

**Inspection
Services
Executives**
Jo Milborrow
Dorothy Wright

**Inspectorate
Risk Manager**
Vacancy

Inspections

GMP/GDP Inspection volumes and performance

MHRA

UK Inspection Programme

- GMP: over **800** sites and **350** Hospital Blood Banks
  - Inspect about **400** sites per year
- GDP: over **3500** sites
  - Inspect about **1000** sites per year

Overseas Routine Inspection Programme

- GMP: over 350 manufacturing sites
  - USA: 163 (last year inspected = 52)
  - **India: 125 (last year inspected = 47)**
  - China: 15 (last year inspected = 3)
  - Total 3rd country last year inspected = 116

Introductory Meeting •Introduction •Major Changes since •Anticipated changes (Personnel, Premises, and Products) •Review of licences – Scope of activities, Range of products •Response to previous inspection •Site master file		Insp 1 QC and Micro •Raw materials •Environmental •Water •Finished product testing •Stability •Retention / Retains •OOS system	Insp 2 Plant rooms •HVACs, •Purified Water •Exterior walk round •Environmental trends •Water trends
Q. Documentation – initial			
Insp 1 •Deviations •CAPA •Recall and Complaints •Vendor management – TSE •PQR process and feedback	Insp 2 •Change Control •Document control SOP •Document completion SOP •Service contracts •Technical Agreements		•Temperature mapping
PM Tour *Insp 1 – focus process - request BMRs BPRs Deviation reps etc* *Insp 2 – focus equip & facility – request calibrations and qualifications etc.* •Starting at Warehouse – materials receipt and sampling •Dispensary through manufacturing •Packaging •Goods dispatch		Insp 1 •Process validation •Batch review / release	Insp 2 •Site VMP •Equipment qualification •Calibration SOP •PPM •Cleaning validation
		•Pest control •Self Inspection •Training •Risk management	
		Close out meeting. - Thanks •Process – Electronic –evidence only on request •Deficiency types - Deficiencies - PIL – Response (28) - Report – GMP Certificate	

What to expect from your inspector

- On time, courteous and abide by site rules e.g. Health and Safety
- Targeted inspection around perceived risk areas
- Pragmatic approach inspecting to a minimum standard
- Systems approach against EU Good Manufacturing Practice Guidelines
- Talk to and challenge personnel at all levels - Give feedback to personnel
- Check for root causes of problems
- Minimum paper work taken from sites
- Investigate action regarding any adverse findings
- Findings should not be addressed / attempted to be addressed while we are on site. Root causes of issues are required to be addressed.

GxP Inspections – Post inspection

Routine
- Post-inspection letter sent, response reviewed, follow-up activities as required
- Inspection report produced, Close out the inspection
- GMP / GDP Certificate / Eudra GMDP

Non routine
- Refer to Compliance Management Team or Inspection Action Group
- An analysis of risk may have to be made by the competent authority
  - Regulatory risk assessment includes factors such as product defect versus product availability versus potential harm to patient
- Outcome of the inspection is the recommendation to the Licensing Authority
- For serious deficiencies potential outcomes may include:
  - Revocation, suspension, variation of licence
    (this may include potential action against Qualified Person)
  - Issue of Statement of Serious Non-Compliance with GMP (SNC) which is visible to all EU member states via EudraLex

Data Integrity:
Overview

- The degree to which a collection of data is complete, consistent, and accurate

*Institute of Electrical and Electronics Engineers

Data integrity from Wikipedia!

Data integrity refers to maintaining and assuring the accuracy and consistency of data over the entire data life-cycle:

- ensure data is recorded exactly as intended
- upon later retrieval, ensure the data is the same as it was when it was originally recorded

Data Life Cycle

- Design of Data Collection
- Transfer of data and meta data

- Objective Processing
- Handling Failures

Data Collection

Data Processing

Data Archive

Data Reporting

Data Review

- Objective Reporting
- Transparency in failures
- Tracking and Trending failures

- Source electronic data
- Re-processing events
- Failures
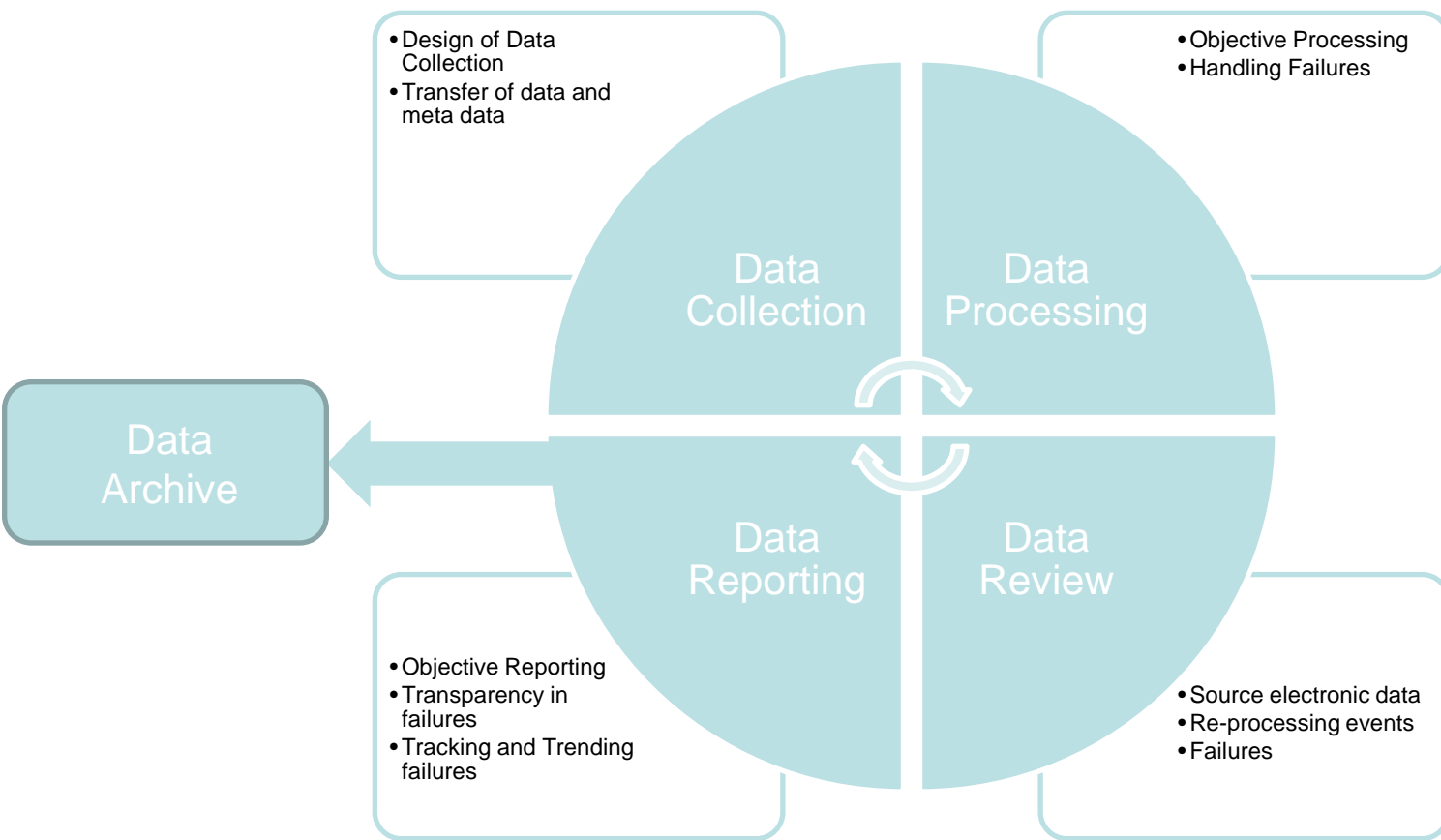
Ref: GMQA

Meta Data   "data about data"

…. information generated as you use technology,

Examples include the date and time you called somebody or the location from which you last accessed your email.

The data collected generally does not contain personal or content-specific details, but rather transactional information about the user, the device and activities taking place.

In some cases you can limit the information that is collected – by turning off location services on your cell phone for instance – but many times you cannot.

Ref: The Guardian

Chromatography Data System

Data – Printed results sheet?

Electronic "data" may include:

Raw data	Result
Method	Sample set
Sequence data	Audit trail files

Ref: GMQA

Data Integrity Issues

2013: increased international regulatory focus on data integrity:

- Global problem

- Potential future change in inspection approach

EU Compilation of Procedures revision to include 'falsification in the context of GMP/GDP'

International regulatory focus

2010 / 2011

US FDA Inspectors received data integrity training

2012

World Health Organisation trained

2013

MHRA with guests from throughout the EU trained

Causes of data integrity issues

Lack of understanding

Willingness to please

Sloppiness

Inadequate Quality Systems to
– Detect, Correct and Prevent

Intentional – data fraud

Ref: GMQA

MHRA

'Tidying' ← → Wilful falsification

'Tidying'

- 'Tidying' often includes changes from original
- Undeclared duplication compromises integrity of <u>all</u> data presented
- Risk that mitigating information becomes less reliable

Wilful falsification

Falsification has no place

in the Manufacture

or Quality Control of medicines

Data Integrity:
Impact

Impact of data integrity issues

MHRA

Impact on Patients

- – Products may be sub standard

- – Resolution of issues may impact on supply
  - Stock shortages

- – Patients may lose confidence in the Manufacturer

Impact of data integrity issues

Impact on Industry

- – Recalls
- – Statement of Non-Compliance
- – Additional regulatory burdens
- – Costs of remediation plans
- – Loss of market share & reputational damage

Reputational Damage

2003 Pan Pharmaceuticals, Australia

Widespread and serious deficiencies and failures in the company's manufacturing and quality control procedures, including the systematic and deliberate manipulation of quality control test data

Reputational Damage

- Batches of medicines on the Australian market recalled

- 219 products identified for immediate recall

- Approval to supply export products cancelled (approximately 1650)

Reputational Damage

On that day

- Hundreds of people lost their jobs

- $350 million was wiped off the Sydney stock exchange

- Scores of businesses, customers and service providers of Pan were very badly affected

Impact of data integrity issues

Personal Impact

- – Job loss
- – Career loss
- – Enforcement action

Personal Impact

MHRA

NEWS EDINBURGH, FIFE & EAST SCOTLAND

2013

< Share

Scientist drug test results

jailed for falsifying

A scientist who faked research data for experimental anti-cancer drugs has been jailed for three months for falsifying test results.

, has become the first person in the UK to be jailed under scientific safety laws.

was working at the Edinburgh branch of US pharmaceutical firm   .   : in 2009 when he came up with the scam.

had been selectively reporting research data since 2003

If it had been successful, cancer patients who took the drug could have been harmed, the court was told.

Edinburgh Sheriff Court heard how   had manipulated the results of an experiment so it was deemed successful when it had actually failed.

Data Integrity:
Self Inspection and reporting

MHRA web alert to Industry: Data governance 16 Dec 2013

- The MHRA is setting an expectation that pharmaceutical manufacturers, importers and contract laboratories, as part of their self-inspection programme must review the effectiveness of their governance systems to ensure data integrity and traceability.

- This aspect will be covered during inspections from the start of 2014, when reviewing the adequacy of self inspection programmes in accordance with Chapter 9 of EU GMP.

- It is also expected that in addition to having their own governance systems, companies outsourcing activities should verify the adequacy of comparable systems at the contract acceptor.

- The MHRA invites companies that identify data integrity issues to contact: GMPInspectorate@mhra.gsi.gov.uk

Self Inspection – where to start?
Are your systems designed to comply

Systems should be designed in a way which encourages compliance with the principles of *contemporaneous record keeping*.

Examples include:

- Access to clocks for recording timed events
- Accessibility of batch records at locations where activities take place so that ad hoc data recording and later transcription to official records is not necessary
- Automated data capture or printers attached to equipment such as balances
- Proximity of printers
- Access to sampling points (e.g. for water systems)

Systems should be designed in a way which encourages compliance with the principles of *contemporaneous record keeping*

The use of scribes to record activity on behalf of another operator should only take place where the act of recording places product at risk
e.g. recording line interventions by sterile/aseptic operators.

Self Inspection – where to start?

Electronic systems:

- Do I have all of my electronic data?

- Do I review my electronic data?

- Does my review of electronic data include a review of meaningful metadata (such as audit trails)?

  - Is this in SOPs? Is it trained?

- Is there proper Segregation of Duties in security access permissions?

- Is my system validated for "intended use"?

Ref: GMQA

What if we find issues?

Weaknesses, if identified early, can be managed as a compliance issue

USE YOUR QUALITY SYSTEM

What if we find issues?

USE YOUR QUALITY SYSTEM

• Raise a deviation

   - must be at a level where QA see it

What if we find issues?

USE YOUR QUALITY SYSTEM

- Conduct and document Impact Assessment
  - Identify the boundaries of the issue
  - If released product is affected
    - inform Marketing Authorisation Holder as soon as possible
    - Ensure the Regulator is informed (Interim Update)

What if we find issues?

USE YOUR QUALITY SYSTEM

- Find and document the Root Cause

- Implement Corrective Actions Preventative Actions

The monitoring and control system

(for computer system reviews and system ownership)

failed to detect loss of control and ensure that the computer validation review system
stayed in a compliant state

(for example through deviation trending)

Data integrity issues

A "special" review project for site validation identified and highlighted the gap in Feb 2013 by which stage the compliance gap appears to have been substantial

On identifying the overall compliance gap no deviation was raised

Data integrity issues

Since identifying the overall compliance gap ongoing non adherence to procedural requirements have not been addressed through the deviation process

The use of the deviation system for departures from procedural requirements within operational IT areas was not routine

Corrective Preventative Actions

Companies need to design Systems and Culture which ensure data integrity

Systems – processes and procedures - that meet the requirements of EU GMP

Culture – No Blame….? Attitude? Approach?

Corrective Preventative Actions

No Blame Culture….? attitude, approach………

Once the Systems are in place

- Personal accountability to follow Policies and Procedures
- Organisation to have a tolerance of mistakes *providing that people learn from these mistakes*

Don't shoot the messenger

Consider a "Notification to senior management" system

Total Quality Management

Open (No Blame?) culture, attitude, approach:

Disparity between:

- 'changing culture' 'encouraging reporting' 'supporting staff' 'no blame reporting' 'training'

and

- 'staff have been told that any data integrity issues will result in dismissal'

You cannot accept staff who *continually, knowingly falsify data*
BUT how can you encourage reporting with a threat hanging?

Total Quality Management

Need a clearly described escalation process

- Reporting

- Training

- Better system design

and then (if continuing), personnel action

Balanced with

"Targets" that are fully defined and appropriately resourced

Properly analysed

Whose responsibility?

Employers need to meet their responsibilities

- Conduct thorough self inspections

- Put in place the measures necessary to ensure good Data Integrity

Whose responsibility?

The person/people doing the self inspection should have knowledge of both the self inspection process and of the potential Data Integrity issues

Cooperation with Personnel is vital

Any required action should be implemented in a timely manner

MHRA web alert to Industry: Data governance 16 Dec 2013

- The MHRA is setting an expectation that pharmaceutical manufacturers, importers and contract laboratories, as part of their self-inspection programme must review the effectiveness of their governance systems to ensure data integrity and traceability.

- This aspect will be covered during inspections from the start of 2014, when reviewing the adequacy of self inspection programmes in accordance with Chapter 9 of EU GMP.

- It is also expected that in addition to having their own governance systems, companies outsourcing activities should verify the adequacy of comparable systems at the contract acceptor.

- The MHRA invites companies that identify data integrity issues to contact: GMPInspectorate@mhra.gsi.gov.uk

Essential: Understand that if you have issues

and have not told us

then the consequences may (potentially) be worse

Misleading your Inspector could lead to a lack of trust
which is very hard to resolve

Agency is aiming to create an environment where
disclosure is more advantageous than concealment

Session 2

Requirements for Data Integrity - Chapter 4 (Documentation)
........as well as a little bit of Chapter 1 and Chapter 6

Corporate Consciousness – Data Integrity

UNCONSCIOUS INCOMPETENCE
Do not know about the issue and unaware of the gap

CONSCIOUS INCOMPETENCE
Aware of the gap but not yet able to deal with it

CONSCIOUS COMPETENCE
Getting a handle on the problem but only with effort

UNCONSCIOUS COMPETENCE
Good practice becomes automatic

Data Integrity:
This is not just a laboratory issue!

MHRA

Training record creation

"caught in the act"

Similar issues with overnight / immediate creation of

- Procedures,
- Change Controls,
- Self inspection programmes

Aim to give the Inspector what they have asked for..?

Likely "Other" deficiency now a "Critical"

Examples of Data Integrity issues

- The site had falsified buildings and documents (in the context of GMP) in that:
  - An office identified as an occupational health centre was then stated as the storage location for the product contact silicon tubing used for the x filling line
  - It was confirmed on the drawings that this office was for occupational health
  - The real general production storage area was not fit for purpose and contained documents that had been falsified

EU GMP

http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm

- Part I   Basic Requirements for Medicinal Products
- Part II   Basic Requirements for Active Substances used as Starting Materials
- Part III   GMP related documents

- Annexes

EU GMP Part 1

Basic Requirements for Medicinal Products

- Chapter 1 Pharmaceutical Quality System
- Chapter 2 Personnel
- Chapter 3 Premise and Equipment
- Chapter 4 Documentation
- Chapter 5 Production
- Chapter 6 Quality Control
- Chapter 7 Outsourced activities
- Chapter 8 Complaints and Product Recall
- Chapter 9 Self Inspection

EU GMP Part 1

Basic Requirements for Medicinal Products

- **Chapter 1 Pharmaceutical Quality System**   **31st Jan '13**
- Chapter 2 Personnel
- Chapter 3 Premise and Equipment
- **Chapter 4 Documentation**   **Jan '11**
- Chapter 5 Production
- **Chapter 6 Quality Control**   **1st Jun '06 (New due in Oct '14)**
- Chapter 7 Outsourced activities
- Chapter 8 Complaints and Product Recall
- Chapter 9 Self Inspection

EU GMP Part II

Basic Requirements for Active Substances used as Starting Materials

EU GMP Part III

GMP related documents

- Site Master File

- ICH Q9 Quality Risk Management

- ICH Q10 Note for Guidance on Pharmaceutical Quality System

- MRA Batch Certificate

- Template for the 'written confirmation' for active substances exported to the European Union for medicinal products for human use

EU GMP Annexes

- Annex 1   Manufacture of Sterile Medicinal Products
- Annex 2   Manufacture of Biological active substances and Medicinal Products for Human Use
- Annex 3   Manufacture of Radiopharmaceuticals
- Annex 4   Manufacture of Veterinary Medicinal Products other than Immunological Veterinary Medicinal Products
- Annex 5   Manufacture of Immunological Veterinary Medicinal Products
- Annex 6   Manufacture of Medicinal Gases
- Annex 7   Manufacture of Herbal Medicinal Products
- Annex 8   Sampling of Starting and Packaging Materials
- Annex 9   Manufacture of Liquids, Creams and Ointments
- Annex 10   Manufacture of Pressurised Metered Dose Aerosol Preparations for Inhalation
- Annex 11   Computerised Systems
- Annex 12   Use of Ionising Radiation in the Manufacture of Medicinal Products
- Annex 13   Manufacture of Investigational Medicinal Products
- Annex 14   Manufacture of Products derived from Human Blood or Human Plasma
- Annex 15   Qualification and validation
- Annex 16   Certification by a Qualified person and Batch Release
- Annex 17   Parametric Release
- Annex 19   Reference and Retention Samples

EU GMP Annexes

- Annex 1   Manufacture of Sterile Medicinal Products
- Annex 2   Manufacture of Biological active substances and Medicinal Products for Human Use
- Annex 3   Manufacture of Radiopharmaceuticals
- Annex 4   Manufacture of Veterinary Medicinal Products other than Immunological Veterinary Medicinal Products
- Annex 5   Manufacture of Immunological Veterinary Medicinal Products
- Annex 6   Manufacture of Medicinal Gases
- Annex 7   Manufacture of Herbal Medicinal Products
- Annex 8   Sampling of Starting and Packaging Materials
- Annex 9   Manufacture of Liquids, Creams and Ointments
- Annex 10   Manufacture of Pressurised Metered Dose Aerosol Preparations for Inhalation
- **Annex 11   Computerised Systems   Jan '11**
- Annex 12   Use of Ionising Radiation in the Manufacture of Medicinal Products
- Annex 13   Manufacture of Investigational Medicinal Products
- Annex 14   Manufacture of Products derived from Human Blood or Human Plasma
- **Annex 15   Qualification and validation   Sep '01 – New in revision**
- Annex 16   Certification by a Qualified person and Batch Release
- Annex 17   Parametric Release
- Annex 19   Reference and Retention Samples

EU GMP Part 1

Basic Requirements for Medicinal Products

- **Chapter 1 Pharmaceutical Quality System**   **31st Jan '13**
- Chapter 2 Personnel
- Chapter 3 Premise and Equipment
- **Chapter 4 Documentation**   **Jan '11**
- Chapter 5 Production
- **Chapter 6 Quality Control**   **1st Jun '06 (New due in Oct '14)**
- Chapter 7 Outsourced activities
- Chapter 8 Complaints and Product Recall
- Chapter 9 Self Inspection

Chapter 1 - Principle

Do not place patients at risk due to inadequate safety, quality or efficacy.

- Responsibility of senior management

- Requires the participation and commitment by staff in many different departments and at all levels within the company, by the company's suppliers and by its distributors

- (vi) Records are made, manually and/or by recording instruments, during manufacture which demonstrate that all the steps required by the defined procedures and instructions were in fact taken and that the quantity and quality of the product was as expected.

Data Integrity - Deficiencies

- ## Non contemporaneous records
  - Batch record not actually available on the packaging lines
  - Kept in IPQA or travels from primary to secondary as they use the same Batch Packaging Record

- ## Inaccurate recording of data
  - Maximum / Minimum Temperature / RH data observed over the limit
  - Records show no previous evidence of Out of Specifications

- (viii) Records of manufacture including distribution which enable the complete history of a batch to be traced are retained in a comprehensible and accessible form;

Destruction of original records

Expectation "neat copy"

We fully accept "scruffy" sets of documentation
when these are the original, contemporaneous ones

If the damage or spillage
(chemicals or text entry boxes limited in size)
means a copy of document is a necessity ....

Expectation "neat copy"

- Have a procedure describing the controls
  - Under the control of Quality Assurance(QA)
  - Subject to a Deviation
- Ensure that the clean "copy" clearly states "copy"
- QA to Second Person Verify the transcription
- Keep the original
- Present both "original" and "copy" sets in an Inspection

1.9 Quality Control is that part of Good Manufacturing Practice which is concerned with sampling, specifications and testing, and with the organisation, documentation and release procedures which ensure that the necessary and relevant tests are actually carried out and that materials are not released for use, nor products released for sale or supply, until their quality has been judged to be satisfactory.

Data Integrity - Deficiencies

Inspectors were informed that the sample worksheets used within the Microbiology laboratory are printed from a stand-alone computer and then the issuance recorded within a logbook.

It was noted that the PDF files for these worksheets had been created on the computer during the inspection, at approximately 18:00 on the 19th February (this was observed in the morning of the 20th February).

The basic requirements of Quality Control include:

- (iii) Test methods are validated

- Peak shaving, during manual integration
- or…adjustment of integration parameters to get the same result

- Under-estimates impurity in related substances testing to bring it within specification

- Turn off integration to ignore 'problem' peaks

Expectation

MHRA
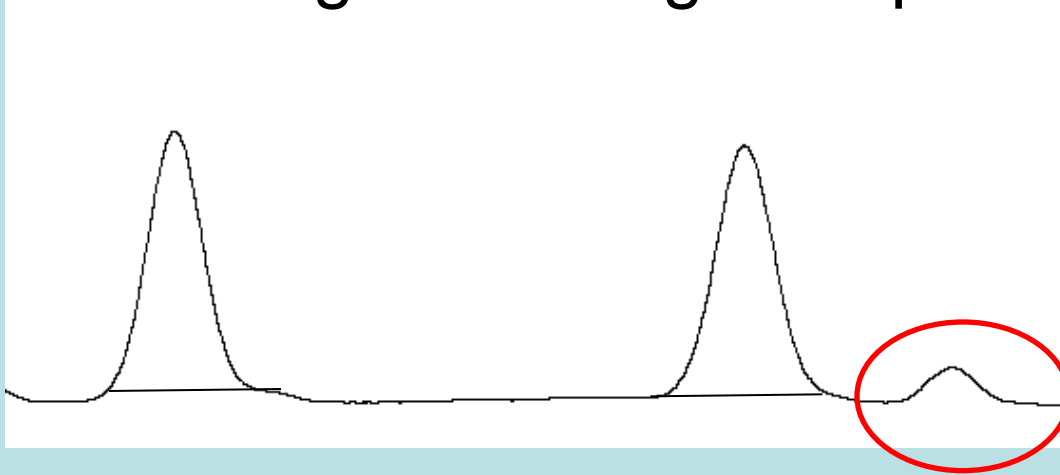
Default position: A validated method for HPLC will not include manual integration

Manual integration should only be used in controlled / approved circumstances in line with a procedure

May be necessary for related substances, large molecules and low level work

The basic requirements of Quality Control include:

- (iv) Records are made, manually and/or by recording instruments, which demonstrate that all the required sampling, inspecting and testing procedures were actually carried out. Any deviations are fully recorded and investigated;

Data Integrity - Deficiencies

There is a failure to ensure that unusual events or deviations are always appropriately investigated:

- The Company attempted six times to test three batches of Product [a].

- Five of the six runs were invalidated but an incident report was prepared on only one occasion.

- The Company violated their own procedure on at least three occasions since the reason for the invalidation of the run was only signed by the operator and not by the Head of QC or their designee.

Data Integrity - Deficiencies

- On 4th September 2013 one of the RT-ID-Test of Product [a] on HPLC [equipment] was not reported at all.

- The data could only be retrieved from the electronic file.

- There was a gap of two hours until the RT-ID-Test of Product [a] was repeated and the test sequence started.

- No explanation was given why this test had been performed and the sequence had not been started immediately after the run but two hours later by a repetition of the RT-ID-Test.

The basic requirements of Quality Control include:

- (vi) Records are made of the results of inspection and that testing of materials, intermediate, bulk, and finished products is formally assessed against specification.

- Product assessment includes a review and evaluation of relevant production documentation and an assessment of deviations from specified procedures;

Data Integrity - Deficiencies

Document review is deficient

The role of "reviewer" within the laboratory lacks an associated Job description, detailed training curricular and a system to ensure the periodic assessment of the practical effectiveness of the training.

Data Integrity - Deficiencies

An appropriate, acceptable standard of record required within the Laboratory has not been clearly identified, issues include but may not be limited to the following:

- There is no formal check of the hard copy report against the soft copy data

- The HPLC hard copy reports do not detail all required metadata (data about data) for example: the integration type

- There is no clear statement that manual integration is not accepted by the Company (or alternately, that only system generated integration is required)

Data Integrity - Deficiencies

The general documentation in the Quality Control laboratory is poor as evidenced by the following:

The records associated with Product [a] were deficient: the official review had failed to address the documentation issues. These include:

Missing entry for calibration due date for [equipment]

Missing entries for a header relating to dissolution which was reportedly blank since purified water had been used and the section was "Not Applicable" but it had not been marked as such.

The balance print out for one of the balances does not include the number for the balance and as such the record cannot be traced.

Principle

- The Quality Management System should include sufficient instructional detail to facilitate a common understanding of the requirements, in addition to providing for sufficient recording of the various processes and evaluation of any observations, so that ongoing application of the requirements may be demonstrated.

Principle

- There are two primary types of documentation used to manage and record GMP compliance: instructions (directions, requirements) and records/reports. Appropriate good documentation practice should be applied with respect to the type of document.

Principle

- Suitable controls should be implemented to ensure the accuracy, integrity, availability and legibility of documents………………… The term 'written' means recorded, or documented on media from which data may be rendered in a human readable form.

Data Integrity - Deficiencies

Excel spreadsheet used to calculate assay:

Date:	28/04/2010	Sample:	T=10
Product Code	FLS 001		Top

Sample Weight   0.9976 g   A
pH   4.23

Date:	28/04/2010	Sample:	T=10
Product Code	FLS 001		Bottom

Sample Weight   2.5599 g   B
pH   4.23

Weight/ml

Corresponding Lab book entries for sample weights:

T=10	2.5813 g	A
M=10	2.5911 g	
B=10	2.5405 g	B

- ***Record/Report type:***

- **Records:** Provide evidence of various actions taken to demonstrate compliance with instructions, e.g. activities, events, investigations, and in the case of manufactured batches a history of each batch of product, including its distribution.
Records include the raw data which is used to generate other records.
For electronic records regulated users should define which data are to be used as raw data. At least, all data on which quality decisions are based should be defined as raw data

- **Reports:** Document the conduct of particular exercises, projects or investigations, together with results, conclusions and recommendations.

Data Integrity - Deficiencies

The Quality Management System lacks adequate controls to ensure a common understanding of the requirements of good documentation practice

Data Integrity - Deficiencies

Records are not always made or completed at the time each action is taken and in such a way that all significant activities undertaken are traceable

ie contemporaneous records to identify who conducted an activity and when

Data Integrity - Deficiencies

There was no awareness that the records for good practice compliance require either a handwritten signature and date or an equivalently controlled record generally with a date stamp within an electronic system

Examples include but are not limited to:

- The Change Control process, including approvers of change proposals
- Approvals of incident management events (Quality Deviations) and associated Corrective and Preventative Actions. (CAPA)
- Qualification records

Good Documentation Practices

4.7 Handwritten entries should be made in clear, legible, indelible way.

4.8 Records should be made or completed at the time each action is taken and in such a way that all significant activities …………… are traceable.

Data Integrity - Deficiencies

The following information was not reported in the Batch Packing Report

- During the inspection tour three operators were standing in the blister packing room where the batch was processed but only the names of two operators were recorded. The name of the third operator who was controlling the cutting of the blisters was not recorded.

Data Integrity - Deficiencies

11 am to 11.43 am.   No blisters were finished on the packing line due to several stops of the machine

Neither the unusual events nor their duration were recorded in the batch packing report at the time they occurred

In addition the entries in the batch packing history card (which were entered after the events had occurred) only mention problems with the feeding channel but there were multiple reasons (e.g. improper sealing and cutting of the blisters) for the stops which were not recorded

Data Integrity - Deficiencies

At least one in process control and test results from 11:38 am have been recorded in the Batch Packing Record that could not have been performed as no blisters were finished on the packing line between 11 am and 11.43 am

Full and accurate documentation of events on the line is essential for both the review of the batch packing record and the subsequent complaint investigations

Good Documentation Practices

4.9 Any alteration made to the entry on a document should be signed and dated; the alteration should permit the reading of the original information. Where appropriate, the reason for the alteration should be recorded.

Data Integrity - Deficiencies

There are records where alterations made to the entries on the documents are not signed and dated

The alterations do not ensure that the original information may be read and they lack explanations for the alterations

Obliteration (including Liquid correction fluid, tape (or stickers) and overwriting) had been used to amend original entries

EU GMP Chapter 4

Retention of Documents

- 4.10 It should be clearly defined which record is related to each manufacturing activity and where this record is located. Secure controls must be in place to ensure the integrity of the record throughout the retention period and validated where appropriate.

Testing

- 4.26 There should be written procedures for testing materials and products at different stages of manufacture, describing the methods and equipment to be used. The tests performed should be recorded.

Data Integrity - Deficiencies

Stability summary reports for Products A, B and C could not be provided to the inspector for review

Nine-month stability results for Product A were reported in the product quality review (PQR) for the period December 2010 to February 2012 however no raw data (in either hard copy or electronic format) could be located to verify the authenticity of these results

Good Quality Control Laboratory Practice

General

6.1 Adequate resources must be available to ensure that all the Quality Control arrangements are effectively and reliably carried out.

Consideration

Formal reconciliation process
for the samples within the Laboratory

to include test samples received, tested and destroyed (to include the routine finished product samples and stability samples)

May protect the company to "know" whether more testing has been conducted than should have been

EU GMP Chapter 6

6.7 Laboratory documentation should follow the principles given in Chapter 4. An important part of this documentation deals with Quality Control and the following details should be readily available to the Quality Control Department:

- specifications;
- sampling procedures;
- testing procedures and records (including analytical worksheets and/or laboratory
- notebooks);
- analytical reports and/or certificates;
- data from environmental monitoring, where required;
- validation records of test methods, where applicable;
- procedures for and records of the calibration of instruments and maintenance of equipment.

6.9 For some kinds of data (e.g. analytical tests results, yields, environmental controls) it is recommended that records are kept in a manner permitting trend evaluation.

6.10 In addition to the information which is part of the batch record, other original data such as laboratory notebooks and/or records should be retained and readily available

The records within the instrument usage log are not comprehensive:

The site run a single point injection of a standard to establish system suitability prior to running samples on the HPLCs. The injection is not recorded in the instrument usage log.

Examples were noted where only one lot identification number was recorded when multiple lots were run.

Not all of the tests which were performed on HPLCx were recorded in the log book

Not all of the batch numbers of Product [a] that were tested between 06th and 07th September 2013 on HPLCy were recorded in the log book (for example, Lot Number xxx was missing).

Unusual events (such as pump leaks, leak detected in instrument etc. on HPLCy between 4th and 5th September 2013) are not recorded at all in the log books.

Consideration

There is a "common practice" of injecting 'trial' injections in HPLC analysis

This seems to be a carry over from R&D
May be used during method development to see whether there's a good chance that the next development cycle will run.

(i.e. before establishing validated analytical parameters).

Please stop this approach in routine manufacture!
………It might be OK for R&D..

6.15 Analytical methods should be validated. All testing operations described in the marketing authorisation should be carried out according to the approved methods.

6.16 The results obtained should be recorded and checked to make sure that they are consistent with each other. Any calculations should be critically examined.

Data Integrity - Deficiencies

The recording of weights of materials tested, from approximately November 2012 to current date, is unacceptable in that there is no second (person) verification of the weights entered into the electronic note book system. As a consequence the results obtained cannot be checked or critically examined.

All testing during the time period is impacted including batch release testing and stability work for nine clinical trial projects. Approximately 60 sets of testing are affected.

EU GMP Chapter 6

6.17 The tests performed should be recorded and the records should include at least the following data:

- a) name of the material or product and, where applicable, dosage form;

- b) batch number and, where appropriate, the manufacturer and/or supplier;

- c) references to the relevant specifications and testing procedures;

- d) test results, including observations and calculations, and reference to any certificates of analysis;

- e) dates of testing;

- f) initials of the persons who performed the testing;

- g) initials of the persons who verified the testing and the calculations, where appropriate;

- h) a clear statement of release or rejection (or other status decision) and the dated signature of the designated responsible person.

6.18 All the in-process controls, including those made in the production area by production personnel, should be performed according to methods approved by Quality Control and the results recorded.

Data Integrity - Deficiencies

Sample name	Acquisition time	Filename
Acet.@250 REP 1	17:13:19	090811-003.rst
Acet.@250 REP 2	17:17:10	090811-004.rst
Acet.@250 REP 5	17:28:19	090811-007.rst
Acet.@250 REP 5	17:34:07	090811-007-20110809-173718.rst
Acet.@250 REP 6	17:37:58	090811-008.rst
Acet.@250 inj acc	17:41:58	090811-009.rst

- Where are REP 3 and REP 4? We have an 11 minute gap and the .005 & .006 datafiles are missing

- Why has REP 5 been reinjected?

- Why does the 6th injection have a different sample name?

Data Integrity - Deficiencies

- On viewing the electronic data the missing results had been run at ~17:21 and ~17:25

- The results had been disregarded

- The HPLC 'passed' the Performance Qualification (PQ) RSD requirement using the amended data set
- The HPLC would have failed the PQ RSD requirement using the original results.

Paper vs Electronic

ALCOA	Paper controls	Electronic Controls
Attributable	Hand signatures Initials	Electronic sign in, log-ons Electronic signature (where used) with associated meaning (Author, Reviewer) Audit trails for create/modify/delete

Paper vs Electronic

ALCOA	Paper controls	Electronic Controls
Legible, Traceable, Permanent	Ink	Controls on overwriting
	No Pencil	Audit trails
	No correction fluid	No "annotation tools" (Electronic correction fluid)
	Rules on crossings out	Archiving, Keeping all records
	Controls and traceability on blank forms (not free issue)	Controls on hidden fields or voided records (access controls, audit trail records)
	No discarding of records	Controls on voiding records
	Archival processes	

Paper vs Electronic

ALCOA	Paper controls	Electronic Controls
Contemporaneous	Dates on Records	Time and date stamps from system clock – Networked or standalone, operating or server clock Time and date stamps are more easily adjusted on un-networked systems. Needs to be traceable to an atomic clock. Synchronisation of clocks between systems. Locking of clocks on PCs if data is captured locally (less of an issue if the PC is just acting as a portal).

Paper vs Electronic

ALCOA	Paper controls	Electronic Controls
Original	Second Person Verification of exact copies of original records. or Retention of original records.	Electronic back up, verification of the back-up should also be in place, either manually or by use of an automated tool. Back-up logs are often maintained but have not been seen in the past as GMP records.

Paper vs Electronic

MHRA

ALCOA	Paper controls	Electronic Controls
Accurate	Direct print out	Records review confirms the accuracy, completeness, content, and meaning of the record) or Documented verification that the printed records are representative of original electronic records (preserving all accuracy, completeness, content and meaning).
	Original records	
		Note .pdf printouts of chromatography records are unlikely to represent a True and Complete copy, due to lack of associated Meta Data and selectivity over what can be printed

Session 3

Requirements for Annex 11 - Computerised Systems
Examples of typical deficiencies

Data Integrity - Deficiencies

When questioned, the site indicated that they were not familiar with the requirements of Annex 11 and data integrity as required by this GMP Annex

Annex 11 - Principle

This annex applies to all forms of computerised
systems used as part of a GMP regulated activities

- A computerised system is a set of software and hardware components which together fulfil certain functionalities.

- The application should be validated;

- IT infrastructure should be qualified.

- Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

- Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality

Consideration

Common for systems to have "initial" classification

GxP – Non GxP – Business critical

If GxP tend to then detail the GAMP Classification

GAMP Classification

1   Infrastructure software including operating systems, Database Managers, etc.

3   Non configurable software including, commercial off the shelf software (COTS), Laboratory Instruments / Software.

4   Configured software including, LIMS, SCADA, DCS, CDS, etc.

5   Bespoke software

Examples of Data Integrity issues

- Access control systems were not validated
  - defined as not a GMP system
  - as a consequence has not been validated

- The building management system has been defined as not GxP
  - There are no procedures defining the access to the system
  - Members of staff which have left the organisation are still recorded as having access

- As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system

Example approach for Risk

New computer system for Electronic Batch records

Justified and documented risk assessment using
High Level Risk Assessment Approach (HLRA)

Assurance of Data Integrity is "built in" to
the Requirements process

1) Functional User Requirements are reviewed and approved by Business Process Owner and Quality Assurance to assure that they reflect the right business and GxP needs

- This ensures that Business process (and therefore data change) steps, including decisions, are defined in the correct sequence, and the important ones (GxP, Business Critical) are identified, in the System URS

- These are subsequently tested by Business Users, and these tests approved by QA Managers

- "High" Risk Requirement are flagged for specific User Testing/SOP creation, in HLRA

Assurance of Data Integrity is "built in" to
the Requirements process

2) User Access Controls

- Each System has an User Access SOP describing the requirement for Training, and proof of need for access prior to approval of Account creation.

- Identity of Users is assured through our Corporate unique personnel ID.

Assurance of Data Integrity is "built in" to
the Requirements process

3) Data Controls

- ER/ES – Rules are included in URS, and tested.

- Password strength – follows an Internal standard, enforced through (a) system itself or (b) User SOP/Training

- Backup and Recovery (inc Disaster Recovery) – always included in URS, and tested.

Basic requirements are set in the URS template

High Level Risk Assessment Approach (HLRA)

Take the Computerised System's

User Requirements Specification (URS) document:

a) Assess the level of Risk associated with each requirement

b) Allocate the suitable Type(s) of Control against each requirement

Example approach for Risk

- Involve Business QA, Business Process/System Owner, IT, and software Supplier staff.
- Usually involves 4-8 people for a workshop lasting 2 days.
- Workshop includes:
  - initial identification of all GxP Requirements
  - analysis of each of these individually, or as a group of related functions.
  - Any other "High" risk requirements will also be individually assessed.
  - Non-GxP or Low Risk Requirements are typically then marked for inclusion in the "end-to-end" testing which will be carried out against the System.

Example approach for Risk
Output
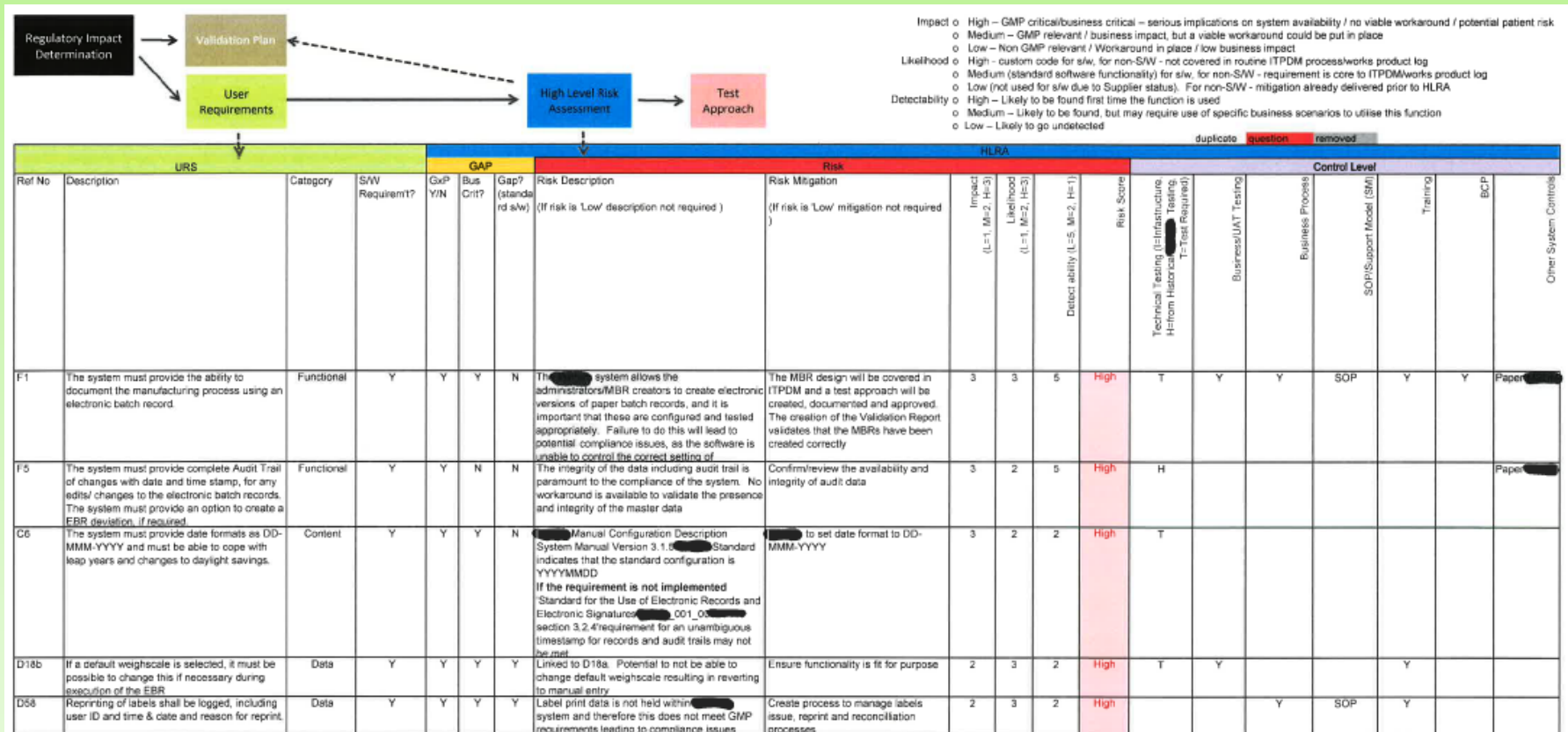
This example was an output of 9 pages

Example approach for Risk

This HLRA technique is essentially a
Failure Mode and Effects Analysis (FMEA) technique

Later in the Project the HLRA table could be used to
produce a Trace Matrix of references to "Controls"

The Template is split into 3 main Sections
(groups of columns):

URS				GAP		
Ref No	Description	Category	S/W Requirem't?	GxP Y/N	Bus Crit?	Gap? (standard s/w)
F1	The system must provide the ability to document the manufacturing process using an electronic batch record.	Functional	Y	Y	Y	N
F2	The system must provide complete Audit Trail	Functional	Y	Y	N	N

Requirement Definition and Characteristics

Green and Yellow columns

- Identity Number, (link from User Requirement)

- Description,

- Whether the Requirement is expected to be met through use of Software

- Regulatory and Business Criticality Flags

-Note as to whether the requirement is actually addressed in the software design or not ("Gap" column)

Example approach for Risk
Section 2 Risk Assessment Scenarios and Scoring

MHRA

	HLRA				
Risk					
Risk Description (If risk is 'Low' description not required)	Risk Mitigation (If risk is 'Low' mitigation not required)	Impact (L=1, M=2, H=3)	Likelihood (L=1, M=2, H=3)	Detect ability (L=5, M=2, H=1)	Risk Score
The ▆▆▆ system allows the administrators/MBR creators to create electronic versions of paper batch records, and it is important that these are configured and tested appropriately. Failure to do this will lead to potential compliance issues, as the software is unable to control the correct setting of	The MBR design will be covered in ITPDM and a test approach will be created, documented and approved. The creation of the Validation Report validates that the MBRs have been created correctly	3	3	5	High
The integrity of the data including audit trail is	Confirm/review the availability and	3	2	5	High

Risk Assessment Scenarios and Scoring

Red Columns

- What could go wrong,

- Scores for Impact, Likelihood and Detectability,

- An overall Score mapped to High/Medium/Low (*H/M/L)*

Failures can be

Functional – failure to perform tasks in the way/sequence expected by the URS/Business Process

Mechanical – functionality may seem ok, but an adverse impact on the platform (e.g. processor overload may occur)

Example approach for Risk
GAMP Guidance (ISPE document) for Risk Scoring and allocation of H/M/L

Impact (of a failure)	
High	GMP Critical /business critical – serious implications on systems availability / no viable workaround / potential patient risk
Med	GMP relevant / business impact but a viable work around could be put inplace.
Low	Non GMP relevant / workaround in place / low business impact
Likelihood (of a computerised system failure occurring)	
High	Custom code for software For non software –not covered in routine IT process/works product log
Med	Standard software functionality for software For non software – requirement is core to IT process/works product log
Low	Not used for software due to Supplier status. For non software – mitigation already in place before risk assessment.
Detectability (of a failure)	
High	Likely to be found the first time the function is used.
Med	May be found but may require use of specific business scenarios to utilise this function.
Low	Low – Likely to go undetected

Factors affecting "Likelihood"

Supplier Status - Set following Supplier Assessment

- Green suppliers tend to decrease the "Likelihood" score, Amber or Red would tend to increase score

GAMP category (3, 4, or 5) of the software

Other factors:

- General Complexity of the Software/Functionality
- "track record" of the supplier

Supplier Assessment
Postal questionnaire or Audit

Green Supplier

- Audited

- Quality Manager and Quality Management System in place

- Trust the Supplier to produce properly Qualified software under their own QMS

Amber Supplier

- Some issues may have been noted in an Audit

- Trust the Supplier to produce software under their own QMS in some areas, but apply additional Controls vs areas of their work with issues identified

Red Supplier

- Several serious issues/inadequacies.

- Typically require the Supplier to follow our QMS, with our Company Quality Approvals

GAMP Classification

GAMP category 3

Software is "standard" / "out of the box" well understood and has been previously deployed to many customers/sites, the "Likelihood of Failure" would tend to decrease

GAMP category 4

Software is "Configurable" the "out of the box" software will have settings applied, from a set of options tested by the Supplier. The software and these configuration settings will be locked down prior to testing and release for use by end users.

for "straightforward" Configuration, or configuration which is very similar to previously proven configurations, the Likelihood would tend to be decreased

for "Complex" or novel configurations, the Likelihood would be increased

GAMP Classification

GAMP Category 5

Software is bespoke this means that the underlying software has been written "to order" for this delivery. The Likelihood would tend to be increased

Technical Testing (I=Infrastructure, H=from Historical Testing, T=Test Required)	Business/UAT Testing	Business Process	SOP/Support Model (SM)	Training	BCP	Other System Controls
T	Y	Y	SOP	Y	Y	Paper
H						Paper

Controls

Light Blue Columns.

Here, the team making the assessment decide which controls are appropriate for each Requirement

High Risk indicates GxP or Business Critical requirement

- Specific Controls (Testing, and/or SOPs) approved by QA will be applied

Low Risk indicates non GxP or Business Critical requirement

- Specific Controls may not be required

This company normally contracts their Software Suppliers to do Technical Testing against all requirements
For Business Testing these requirements will be included in "End-to-End" Test scenarios as a minimum

Example approach for Risk

Example Controls would be

- Technical Testing and User Testing (individual function or "end-to-end"),

- Manual Control,

- Standard Operating Procedures/ Application Support Model,

- Training,

- Business Continuity Plan,
or passing control to another System

Example approach for Risk
Controls terminology

- Technical Testing (individual function or "end-to-end")
    - Testing to check that the built software meets its Design Specifications and is stable in use
    - Executed by the software supplier, and approved by a Company IT Quality Manager
- User Testing (individual function or "end-to-end")
    - Testing to check that the built software meets the User Requirements and data flows and values meet the expectations of the Business Process
    - Executed by the Business Staff, and approved by a Production QA Manager
- Manual Control
    - For Business Process steps NOT supported by software, manual steps may be required. Also applies to activities such as e.g. approving a User to be allowed an account on the computer system. These activities should be defined in SOPs (below) and should be tested as part of "end-to-end" System Testing
- Standard Operating Procedures/ Application Support Model
    - To support Manual Controls
    - SOPs should be owned and signed off by Business Process Owner (BPO) or System Owner, and a Production QA (if activities are GxP)
    - Support Model should be backed by Service Level Agreements, and approved by IT Quality Manager
- Training
    - Owned by System Owner, aligned to Roles, Approved by Business Process Owner
    - System Owner must have a process to ensure that Training is delivered before User accounts are granted
- Business Continuity Plan, or Passing control to another System

Example approach for Risk

The HLRA process will identify a number of Controls for the System

Following the HLRA, the following documents may be updated:

- Validation Plan (if significant SOPs, or tests including other Systems, are identified)

- Test Approach

- Change Requests vs other Systems (if identified during the HLRA)

- Traceability Matrix – this will be created and populated with references to actual Test Scripts, SOPs etc.

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT.

All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Data Integrity - Deficiencies

The Laboratory System Administrators
are within the Quality Control team
and as such have
inappropriate administrative access
to all of the Laboratory software.

3.1 When third parties (e.g. suppliers, service providers) are used e.g.

to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing,

formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party.

IT-departments should be considered analogous.

Data Integrity - Deficiencies

The vendor management system holds details of the software suppliers but there is no clear oversight mechanism to demonstrate that valid formal agreements are in place with the key software suppliers.

Data Integrity - Deficiencies

There is a lack of formal record as to which organisation has the current responsibility for a software system.

For example.
Equipment within the *Building A* areas were initially *supplier B* systems and it is this organisation that is identified in the CSV system.

Supplier B has gone out of business, and it is now the responsibility of Site IT department to look after that software. This is not formally stated within the records relating to the system (such as within the CSV system or perhaps in the SAP maintenance module).

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider.

The need for an audit should be based on a risk assessment.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

Data Integrity - Deficiencies

The Qualification of laboratory systems failed to appropriately address data integrity considerations

Deletion of GMP-relevant data is possible and no documented records are available to support the deletion

- Data had been deleted from HPLC (result files deleted by the administrator)

- Data had been deleted from UV spectrophotometer

.

Whilst tasks such as Qualification may be contracted out to Suppliers it remains the responsibility of the User to ensure that the set up is suitable for their requirements.

Computerised systems should comply with the requirements of EU GMP Annex 11 and be validated for their intended purpose

This requires an understanding of the computerised system's function within a process

For this reason, the acceptance of vendor-supplied validation data in isolation of system configuration and intended use is not acceptable

In isolation from the intended process or end user IT infrastructure, vendor testing is likely to be limited to functional verification only, and may not fulfil the requirements for Performance Qualification.

For example - validation of computerised system audit trail

- A custom report generated from a relational database may be used as a GMP system audit trail.

- Procedures should be drafted during Operational Qualification to describe the process for audit trail verification, including definition of the data to be reviewed.

- 'Validation for intended use' would include testing during Performance Qualification to confirm that the required data is correctly extracted by the custom report, and presented in a manner which is aligned with the data review process described in the SOP.

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

Data Integrity - Deficiencies

MHRA

The IT representative indicated inspection reports of suppliers would not be available since to supply them would be contrary to management procedure.

The Inspector indicated that the company would have to change their management procedures.

The Head of QA concurred and there were no issues in obtaining the required documents.

Annex 11 – Project Phase
4. *Validation*

4.1 The validation documentation and reports should cover the relevant steps of the life cycle.

Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

Data Integrity - Deficiencies

- The system that manages the building management (HVAC etc) is not included in the list of computer systems.

- As a minimum the system should be identified, secure and procedures in place for the operation and appropriate access rights assigned.

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

Annex 11 – Project Phase
4. *Validation*

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.

For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

Data Integrity - Deficiencies

- The listing of all relevant GMP systems and their GMP functionality is deficient in that:

- The list is not a current, accurate list and the GMP functionality of the systems is not included / apparent

This site had a list of all computer systems

in excess of 600 systems (down from 800+)

which they presented when asked for their listing of GMP Systems but it included "all sorts" – some of which were no longer in place

4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact.

User requirements should be traceable throughout the life-cycle.

4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system

4.7 Evidence of appropriate test methods and test scenarios should be demonstrated.

Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

Annex 11 – Operational Phase
5. *Data*

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

Expectation

Are all relevant systems interfaced and have the interfaces been validated?

- e.g. analysis systems and LIMS

System checks may automatically confirm data transfer –for example, Backup checksum

Annex 11 – Operational Phase
6. *Accuracy Checks*

For critical data entered manually, there should be an additional check on the accuracy of the data.

This check may be done by a second operator or by validated electronic means.

The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management

Data Integrity - Deficiencies

The procedure for the use of Excel spread sheets lacked a clear statement that the manually entered data requires an additional check on the accuracy of the data input.

Checks should be attributable

Truly critical checks should be "blind"

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

Expectation

Backup media

- Sites frequently use removable media (e.g. tapes / CD's) and store them in a fireproof safe but do not control or monitor the temperature and Rh. The integrity of the backup data is thus questionable.

- Removable media does have defined lifetime with specified storage requirements, e.g. for backup / archive of tapes, typically 5ºC to 23ºC/20%Rh to 50%Rh. This is generally stated on the tape cover / insert.

8.1 It should be possible to obtain clear printed copies of electronically stored data.

8. *Printouts*

8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry

Data Integrity - Deficiencies

The electronic data of the HPLCs [1] and [2] could not be retrieved during the inspection.

- There is no way for these records associated with Batch release to be printed indicating if any of the data has been changed since the original entry.

Annex 11 – Operational Phase
9. *Audit Trails*

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").

For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

Expectation

Continuum of complexity of instruments
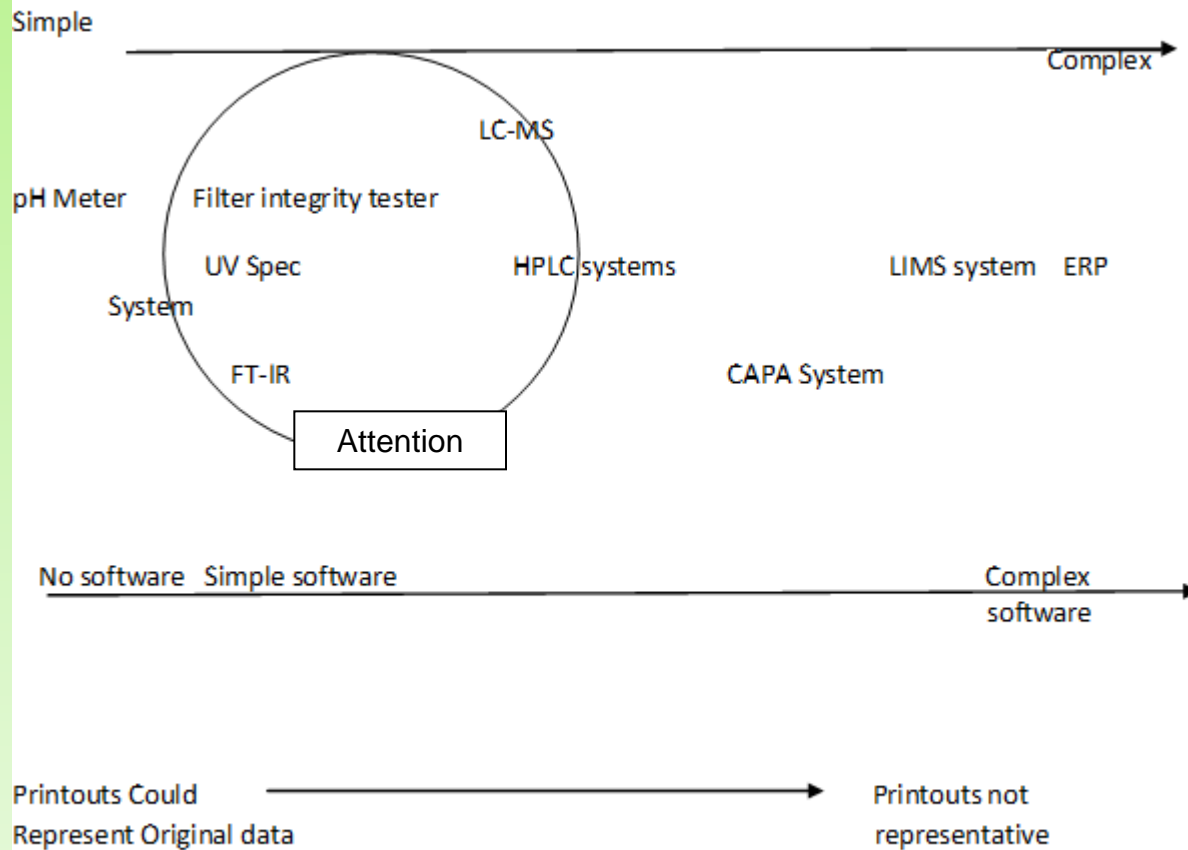
Ref: GMQA

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure

Annex 11 – Operational Phase
11. *Periodic evaluation*

- Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.

- Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

Data Integrity - Deficiencies

Periodic evaluations are required for all computer systems (based on the criticality identified in the risk assessment).

There is no system for this process to confirm that the systems remain a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

The periodic review of computer systems asks if the System owner believes that the validated status of the system has been maintained based on the number of Change controls.

Such a statement should be based on the Number and Type / Criticality of changes – not number alone.

Annex 11 – Operational Phase
12. *Security*

12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons.

Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

12.2 The extent of security controls depends on the criticality of the computerised system.

12.3 Creation, change, and cancellation of access authorisations should be recorded.

Expectation

MHRA

Check the Access for relevant computerised systems

- Individual user login
  - Sites have been found to have generic logins, mainly on the basis of not having to buy additional licences to enable individual login.
  - This is not acceptable if the software version includes the facility for individual login.

- User / group permissions
  - May be too extensive. May permit lower level users to delete or modify data files / configuration settings / method files?

12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

Data Integrity - Deficiencies

- The system settings for two computer systems associated with on site chromatography have not been set to ensure GMP compliant records are created.

- System [1] has the general setting "Save all analysis results." This option is currently disabled

- As a consequence of this option being disabled only the original and most recent result will be saved in the file. The multiple re-processing of analysis cannot be viewed.

Data Integrity - Deficiencies

System [2]

- The software providers recommendation for regulated users highlighted as 'GxP' had not been checked as required.

- "Disallow use of Annotation tool." This option is not currently enabled.

- As a consequence of this Policy failing to be enabled all Analysts have the potential to generate paper / hard copy reports which can be printed with original data and information be masked or overwritten.

- *Note: The soft copy will remain as was and such activities ought to be detectable during review of the soft copy data.*

- All incidents, not only system failures and data errors, should be reported and assessed.

- The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,

b. be permanently linked to their respective record,

c. include the time and date that they were applied.

15. *Batch release*

- When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches.

- This should be performed using an electronic signature.

- For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system).

- The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports.

- These arrangements should be adequately documented and tested.

- Data may be archived.

- This data should be checked for accessibility, readability and integrity

- If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested

Expectation

Are the audit trails backed up?

- Sites often back up method / analysis files, but not the audit trail.

- Check Data files / configuration settings / method files?

Session 3

- **Is compliance to 'Annex 11' sufficient to prevent 'Data Integrity Issues'?**

'Tidying'

Wilful falsification

Data Integrity - Deficiencies

Sample name	Acquisition time	Filename
Acet.@250 REP 1	17:13:19	090811-003.rst
Acet.@250 REP 2	17:17:10	090811-004.rst
Acet.@250 REP 5	17:28:19	090811-007.rst
Acet.@250 REP 5	17:34:07	090811-007-20110809-173718.rst
Acet.@250 REP 6	17:37:58	090811-008.rst
Acet.@250 inj acc	17:41:58	090811-009.rst

- Where are REP 3 and REP 4? We have an 11 minute gap and the .005 & .006 datafiles are missing

- Why has REP 5 been reinjected?

- Why does the 6th injection have a different sample name?

Data Integrity – Issues: Understanding and Resolution

- Do I have all of my electronic data?

- Do I review my electronic data?

- Does my review of electronic data include a review of meaningful metadata (such as audit trails)?

  – Is this in SOPs? Is it trained?

- Is there proper Segregation of Duties in security access permissions?

- Is my system validated for "intended use"?

Corporate Consciousness – Data Integrity

UNCONSCIOUS INCOMPETENCE
Do not know about the issue and unaware of the gap

CONSCIOUS INCOMPETENCE
Aware of the gap but not yet able to deal with it

CONSCIOUS COMPETENCE
Getting a handle on the problem but only with effort

UNCONSCIOUS COMPETENCE
Good practice becomes automatic

Acknowledgements

David Churchward, Expert GMDP Inspector, MHRA

Mark Webb, GMDP Inspector, MHRA

Monica Cahilly, Green Mountain Quality Assurance LLC, info@GMQA.net

R.D. McDowall, Article - US FDA's Focus on Laboratory Data Integrity

The Guardian Newspaper

Mark Cherry

GAMP 5 "Risk Based Approach to Compliant GxP Computerised Systems" ISPE

© Crown Copyright 2014