Computers and E-documents in a regulated environment

David R Buckley FQSA

info@navigategmp.com

enquiries_dba@optusnet.com.au

Introduction

- TGA
  - 2005 name change A&NZ – "Pharmaceutical Products"
- Therapeutic Goods Act 1989
  - Licence requirements and conditions
  - Manufacturing Principles
    - Code of GMP – same as PICS but!
      - " Should" and "shall" mean "must" ie "mandatory"
      - Annex 5 (EU – 11) computers, Annex 15 – validation (includes laboratories)
- TGA MAS Auditors
  - Powers of entry
  - Training
  - Specialists

Regulators

- USA - FDA increasing scrutiny
  - Expectations
  - Freedom of Information
  - Consent decree
- Europe - changing
  - UK MCA, keeping pace with and influenced by the FDA
  - Tends to set bench mark for Europe
  - Freedom of Information in preparation
- Japan - imported drugs are under scrutiny
- Australia - TGA using European GMP but tending to FDA interpretations
  - FOI but never really tested for inspection reports
  - Independent product review

FDA consent decrees

Wyeth October 4, 2000

- $15,000 per day if fail to adhere to corrective action schedule (up to a $5,000,000) and
- Pay $30,000,000 to U.S. Treasury

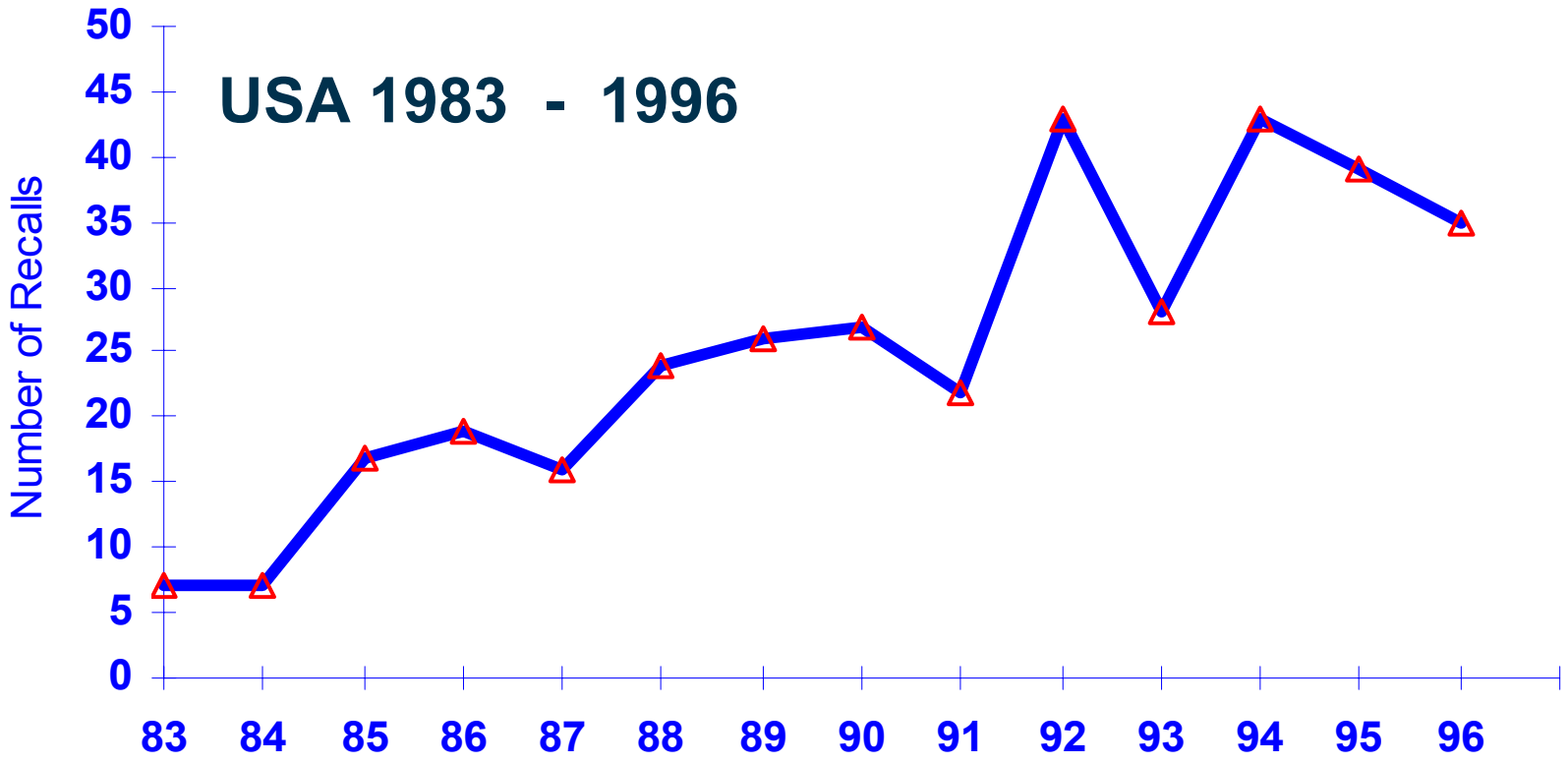
Abbott November 2, 1999

- $15,000 per manufacturing process, per day, (up to $10 million dollars cap) if fail to adhere to corrective action schedule and
- Pay $100,000,000.00 to U.S. Treasury

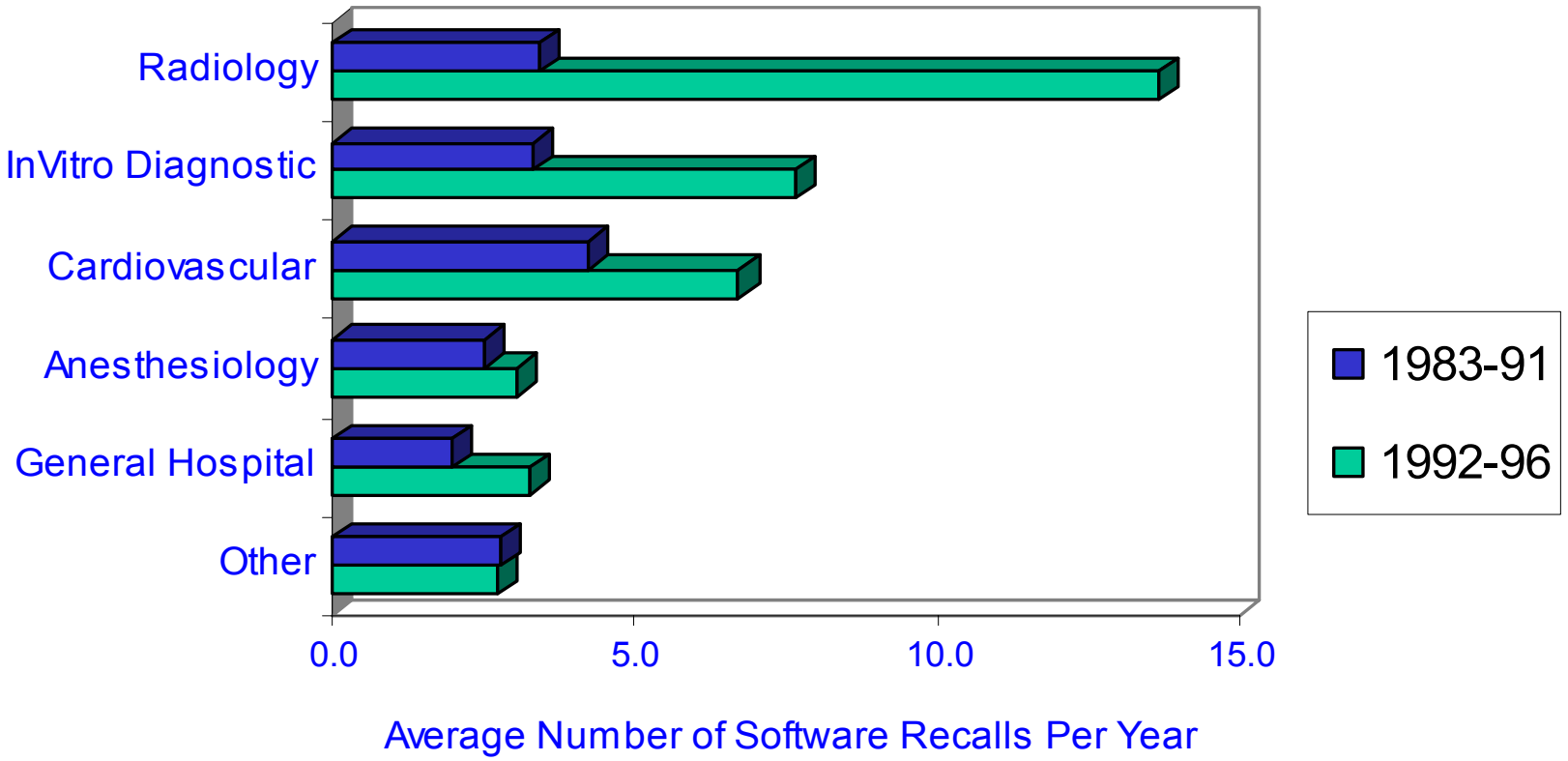
Schering-Plough May 20, 2002

- Pay $500,000,000.00 to U.S. Treasury

Medical device software associated recalls



US Device Software Recalls



Regulatory Action

Once a company is found deficient:

- Corrective action is difficult, long, very costly
- Affects all parts of the business
  - Interruption of market supply
  - Independent product review
  - Loss of reputation
  - Loss to shareholder of stock value
  - Financial implications
  - Major company re-organization
- All parts of TGA get involved

Regulatory Inspections

Navigate GMP with DBA

Key Regulators are:

- Becoming more “risk averse”
  - No risks - no mistakes
- Introducing Quality Systems approach to inspections
  - PIC/S
- FDA requiring companies to make “global commitments” on behalf of all sites
  - Wyeth
- FDA Issuing Warning Letters to Pharmaceutical, Consumer Healthcare Companies
- TGA unannounced audits
  - During normal business hours also means 1230pm!
  - Teams of 3 or 4
  - Auditors with specialist skills

The major risk areas

- USA - FDA increasing surveillance and expectations
- Europe - rapidly changing
  - UK MCA, keeping pace with and influenced by the FDA, sets standards for Europe
  - Has established a “merged company” database
  - Moving towards Freedom of Information
- Japan - imported drugs are under scrutiny
- Australia - TGA using FDA standards
  - Changes post Pan

TGA and Industry need …

•.... confidence in the production and management computers and electronic records

•.... Proof of a capable system

•.... Evidence that computer systems are fully validated

•.... Ability to obtain true and accurate copies of e-records, both electronically and on readable hard copy (now and into future)

•.... “Secure” e-records and traceability

•…. Applies to all systems involved with manufacturing

E-doc

Applies to

- Custom/Commercial/Proprietary Software (OTS, COTS)
- Electronic Batch Records
- Laboratory Analysis Data
- Facility Design Documents
- Records
  - Maintenance
  - Cleaning
  - Calibration
  - Deviations, OOS
- Procedures
- Product Label Information
- Spreadsheets/Databases
- Validation Records

Controls

- Policy for operation/responsibilities of system owners
- Computerised system requires validation
- System to be secure, with appropriate access controls
- Authority/device checks for input data
- Sequence step control (process control systems)
- Training of developers and operators
- Controls over system documentation
- Change control
- Audit trail
    - -Time stamped
    - -Unable to be altered
    - -Computer generated
    - -Not accessible by operator

Code comparison

Navigate GMP with DBA

21 CFR part11 Electronic Records, Controls for Closed Systems		EU GMP Annexe 11 Computerised Systems	GAMP Appendix 4 APV Guideline
Validation	11.10a)	11.2, 11.7, 11.19	2, 2.1, 4
Copies of Records	11.10b)	11.12, 11.13	5
Record Protection	11.10c)	11.13, 11.14, 11.15, 11.16	5, 2, 2.1, 6
System Access	11.10d)	11.8, 11.19	3, 4
Audit Trails	11.10e)	11.10, 11.19	4
Sequencing	11.10f)	11.6, 11.19	4
Authority Checks	11.10g)	11.8, 11.9, 11.10	3, 4
Device Checks	11.10h)	11.6, 11.9	2.1, 4
Training	11.10i)	11.1	1.3
Policies	11.10j)	11.19	4
Document Controls	11.10k)1)	11.16, 11.17	2, 2.1, 6
Change Control	11.10k)2)	11.11, 11.17	2, 2.1, 6

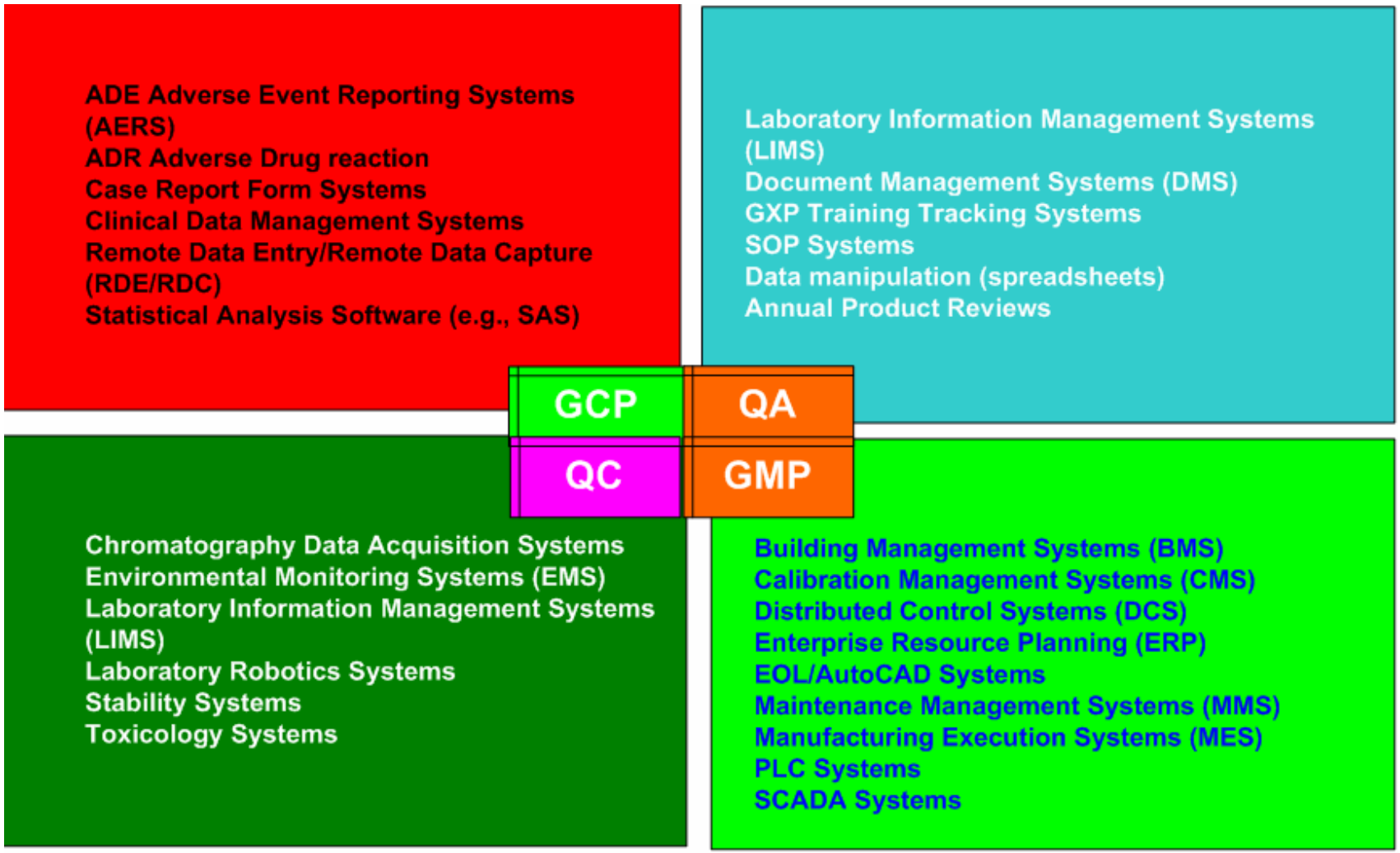
Pharma E-docs

Navigate GMP with DBA

- US 21 CFR part 11 applies to:
  - Records in electronic form required under any pre-existing FDA regulation (FDA “predicate rules” for gmps, glps, gcps)
  - Electronic records submitted to and subject to inspection
  - Hardware, software, documentation associated with both
  - Includes hybrid systems, electronic records that do not include an electronic signature
  - Computer controlled manufacturing processes

Pharma E-docs

Navigate GMP with DBA



Pharma E-docs - definitions

Navigate GMP with DBA

- **Electronic record**
  - any combination of ***text, graphics, data, audio, pictorial, or other information***…in digital form that is "created, modified, maintained, archived, retrieved or distributed by computer system"
- **Electronic signature**
  - A computer rendition (biometrics, non-biometrics, digital) of some unique 'mark' that an individual ***executes, adopts and authorises*** that is considered to be a legally binding equivalent of a handwritten signature

- **Closed system**
  - an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system
- **Open system**
  - an environment in which system access is not controlled by persons responsible for the content of the electronic records on the system

Pharma E-docs - definitions

- **Volatile (transient) vs nonvolatile data**
  - Volatile data - Electronically gathered but not archived on electronic media for future retrieval
  - Nonvolatile data - Electronically gathered & stored on durable media, even for short periods of time
- **Validation**
  - accuracy
  - reliability
  - consistent intended performance
  - ability to discern invalid or altered records (audit trails)

Audit Trails

- All changes must be recorded
- Available for inspection and copying
- Computer generated
- Date and time stamped
- Does not obscure previous data
- Independently recorded
- Retain for full retention period
- Attempts of unauthorised access recorded
- Should not be able to be viewed by operator

Pharma E-docs

Navigate GMP with DBA

Security

- System access is limited to authorized individuals; authority checks must be conducted to grant access and/or sign an e-record

Retention

- must be available throughout the records retention period (governed by predicate rule)

Copies

- must be available in both human-readable and electronic form

Training

- Assurance that persons who develop, maintain or use E-dco systems are properly trained
- utilize vendor audit program and in-house training programs for evidence

Documentation Management programs

- vendor documentation
- in-house documentation
- change and revision control on both

Pharma E-docs

Navigate GMP with DBA

1. Written Policies
    - defining individual accountability and responsibility for actions initiated under individual's e-signatures and e-identity
2. Operational System Checks
    - forced sequencing of steps, like a workflow or EBR
3. Device Checks
    - to determine validity of source data
4. Open versus closed systems
    - both subject to the e-records requirements
    - open systems must apply additional controls to assure data integrity such as encryption and digital signatures

Electronic Signatures

Navigate GMP with DBA

- Unique
  - Unique to an individual
- Not reused or reassigned to anyone else
- Individual's identity verified prior to signature authority
- Prior to or at time of use, for FDA, the organization must certify to the Agency that e-signatures are the legally binding equivalent of handwritten signatures
- Must contain
  - printed name of signer
  - date and time when signing executed
  - meaning associated with signature
  - must be readily readable (by a human!)
- Must be unbreakably linked to associated electronic record
  - Must not be able to be copied, excised or otherwise utilised to falsify a record

Electronic Signatures

Navigate GMP with DBA

- Nonbiometric signatures comprised of at least two distinct components
- Must be used only by genuine owners
- Must be managed
  - Use of one person's e-sig by another fraudulent behavior
- Combination of ID and password constitutes uniqueness
  - must be maintained
- Continuous signing events allow the use of only one component during the signing period
  - session must be opened with full signature
  - otherwise all signing events considered discrete & all e-sig elements must be used
- Password aging
- Loss management of tokens or other identity-bearing devices
  - Include a program for replacements
  - Need a testing program to determine that devices perform properly
- Intrusion detection
  - Include the use of transaction safeguards (3 strikes)
  - Detecting and reporting "in an immediate and urgent manner" attempts to sign a record or use a system without having proper access
  - Report attempts to system security and/or organizational management

Computer validation requirements

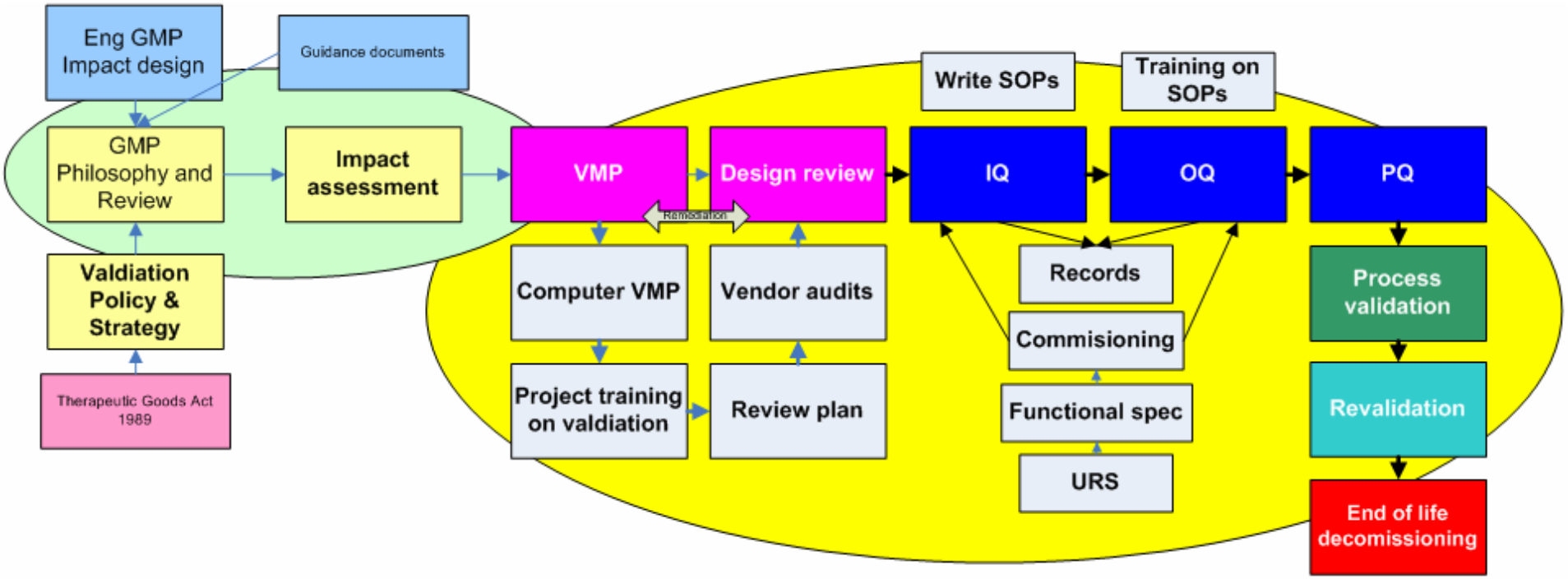
1. Closed System
2. Generation of copies of records
   - human readable and electronic
3. Protection of records
4. Limited System Access
5. Use of audit trail
6. Operational System Checks
7. Authority checks
8. Key signature requirements
   - Printed name of signer
   - Date and time
   - The meaning
9. Signature controls
10. Signature uniqueness - can not be “copied”
11. 2 distinct identification components
12. Uniqueness of Passwords and ID’s
13. Safeguards to prevent unauthorized use
14. System Validation

Validation

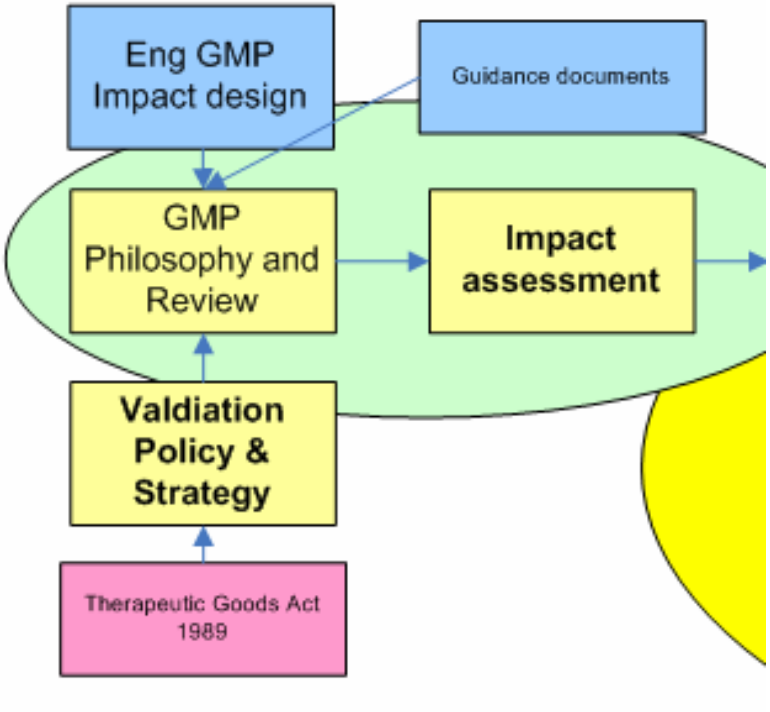
- Validation plan
  - defines strategy, responsibilities, approach, tasks
  - signed by management
- Validation procedures/protocols
  - how will the testing be carried out and documented?
- Validation reports - the collated efforts of the testing, specifying quantifiable results rather than qualitative as much as possible
- Hardware and software IQ
  - OS
  - data base
  - application

Validation expectations

Navigate GMP with DBA



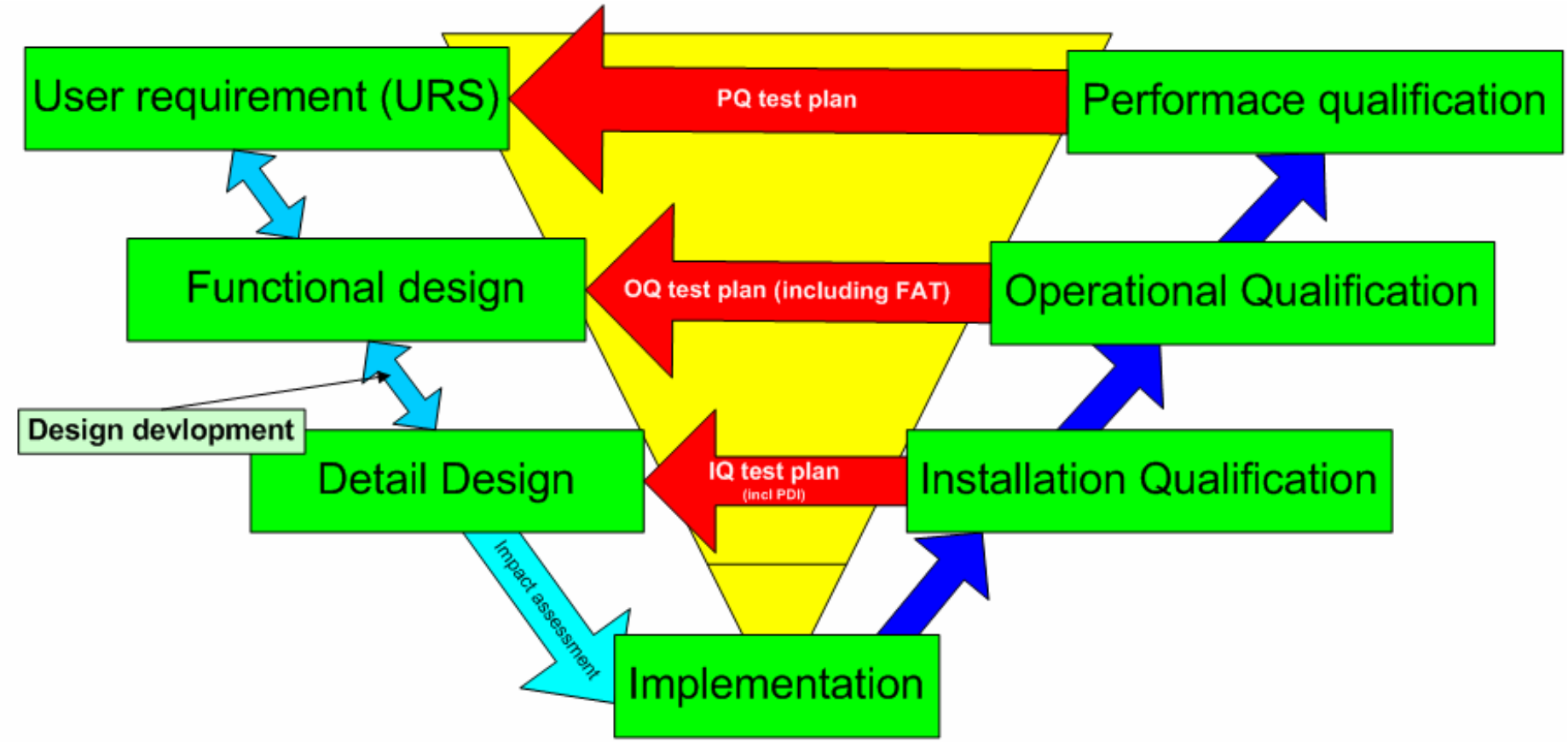
Not generally audited



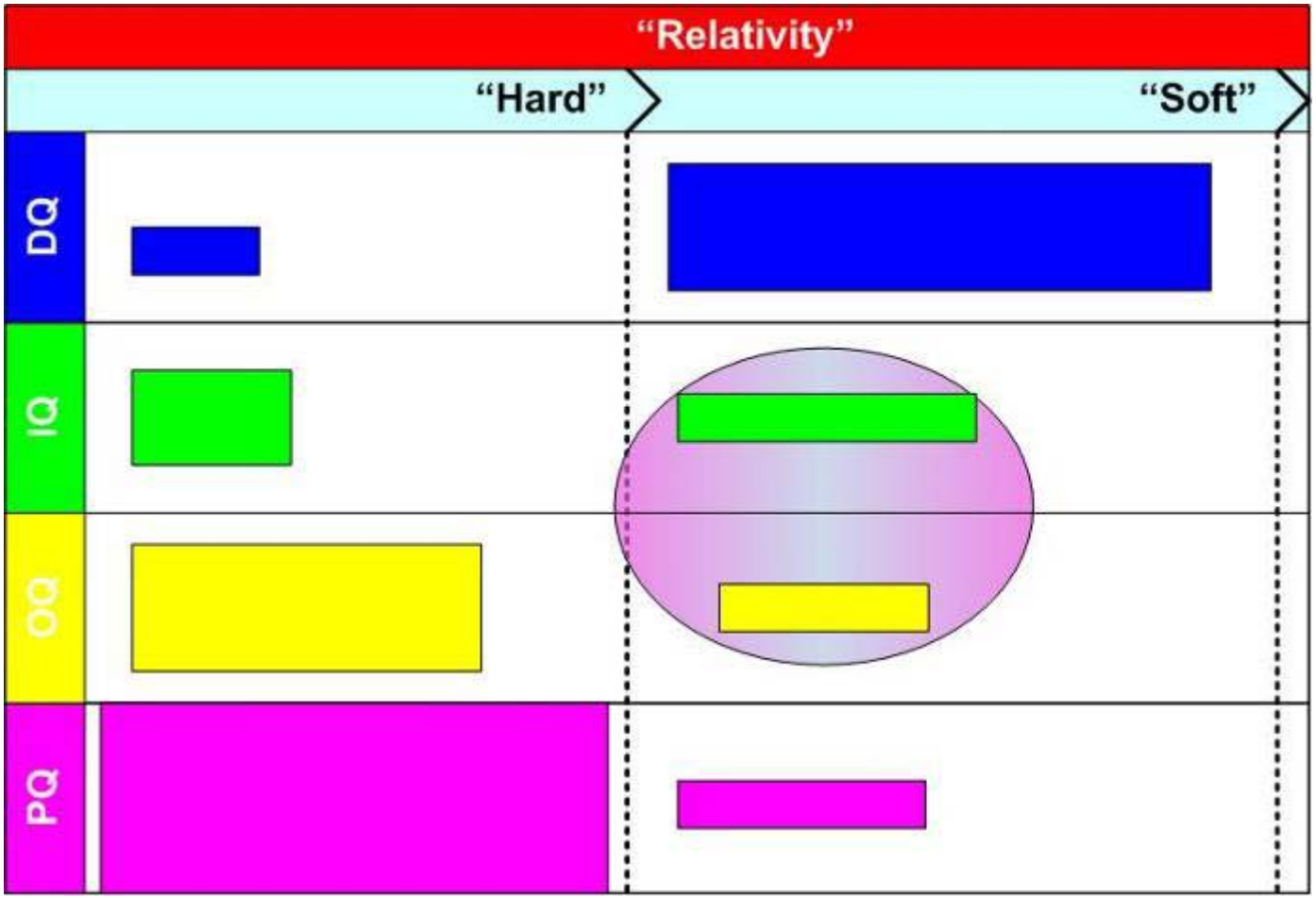
Generally subject to audit

Navigate GMP with DBA

V-model



“Relativity”



URS requirements

- Each requirement uniquely referenced
- Requirement statements not duplicated nor contradicted
- URS should express requirements **not** design solutions
- Each requirement should be testable or verifiable
- The URS must be understood by both user and supplier:
  - Avoid ambiguity and jargon
- Requirements should be prioritized
- URS should distinguish between essential requirements and merely desirable features.

Item	Function Name	Function Description	21 CFR 11
01	Copy of records	Records copy (audit trail, batch report)	11.10. b
02	PDF files	Reports converted to PDF standard	11.10 c
03	Limited system access	Limit system access to authorised users	11.10 d, 11.10 g
04	Audit trail	Generation of an Audit trail	11.10 e
05	Record changes	Previously recorded info still visible	11.10 e
06	Storage	Storage / archiving of Audit trail data	11.10 e
07	Signature	Signature manifestation	11.50 a 1 – 3
08	Signature record linking	Signature record linking enabled	11.70
09	Uniqueness of combo	Uniqueness combo UID & password	11.100 a, 11.300 a
09	UID in barcode	Unique ID + password, UID in barcode	11.200 a 1
10	Series of signing	Series of signing, subsequent signings UID (barcode) should be used	11.200. a 1 I
11	Password aging	Password change after x time	11.300 b
12	Logout	Automatic logout after x minutes	11.200 a 1 II
13	Unsuccessful logins	Unsuccessful logins documented	11.300 d
14	Blocking of user	Block user after x unsuccessful logins	11.300 d
15	Intrusion, attack	Compare system after with before	11.300 d

Validation

- Dynamic testing
  - normal as well as stress conditions to include boundary testing, errors, etc
  - simulation - conducted offline
  - live, user site - under actual, continuous operating conditions
  - structural - white box to show that the software creator followed SDLC (code reviews)
  - functional - black box to show that inputs yield expected outputs
- Static testing
  - document and code inspections
  - code walk-throughs
  - technical reviews
- Extent of validation
  - based on risk system poses to product safety, efficacy and quality, data integrity/authenticity/confidentiality, system's complexity

Validation

- Results review must be independent of execution
- Configuration management must be in place to include firmware changes, service packs, bug fixes
- COTS (no access to source code)
  - validate custom changes
  - review of software performance history
  - perform software vendor assessment
- Internet
  - CAN'T BE VALIDATED!!
  - validate data source
  - data destination environments
  - consider additional measures to assure integrity and authenticity
    - eg digital signatures
    - delivery acknowledgements

IQ Requirements

Navigate GMP with DBA

- System description
- List of applicable specifications
- Hardware components list
- System software configuration list
- Application software configuration list
- Fixed configurable data list
- Electrical power requirements
- Installation and hook-up inspection
- Documentation requirements
- Calibration requirements
- Preventative maintenance requirements
- System training
- Deficiency reports

OQ requirements

- Calibration verification
- Input/output verification
- Program functional test
- Screen tests
- Alarm challenges
- Program security challenges
- Power failure recovery
- Backup and recovery
- RFI testing
- EMI testing
- Report format verification
- Check against operating procedures

PQ requirements

- System challenges against URS
- Worst case condition challenges
  - Memory
  - Capacity
  - Multi terminal access
  - Users
- Boundary and extreme value challenges
- Abnormal pathway challenges
- Positive and negative tests

Audit trail

- Time stamps must be based on computer system clocks
  - Accurate
  - Reliable
  - Ideally automatically synchronized to a “master clock”
- Clock functions
  - Security to prevent unauthorized changes or/and coupled with employee training where technical restrictions are not available (laptops)
- “Time stamp policing” - unannounced checks of computer clocks, spot checking audit trail time stamps for anomalies
- Time zones - “local time” dilemma - often server time
- Assure organization understands how date and time are expressed

Maintenance

- E-records must be available and readable throughout the record retention period
  - Select media carefully – Stability? Recovery? Reading hardware?
  - Have a data recovery process for retrieving information from old media
  - Backups of archive media
- Must be stored under conditions that will not accelerate media deterioration
  - EMF
  - EMR
  - Process should be validated if there is no built in error-checking
- Approaches to assuring continued e-record availability
  - Save everything
    - hardware
    - software
    - continue to train staff on the system use, even if system no longer used for production
  - only short term needs

Maintenance

- Migration – move records from one environment to another
- Retire or discard old system after reasonable period (?)
- Assure continued e-record integrity and reliability
  - take into consideration
    - moving from one OS to another
    - one type of storage media to another
    - one file format to another
    - one type of peripheral to another
- consider use of third party authentications
- include controls over data, metadata, hardware, software, audit trails, e-signature links as part of migration process
- After migration should be able to “search, sort and process information in the migrated electronic record at least at the same level as what you could attain in the old system”

Electronic Copies

- Have to be accurate and complete but not necessarily in the same format at they were created
  - Accurate and complete means including audit trails, metadata and e-signatures
- Validate the copying process
  - Include considerations of file format, media, built-in error-checking capabilities
- Any hyperlinked reference is considered part of the copy
- E-copies of the database queries used to retrieve the copy information should be included with the e-record
- E-copies should carry some form of authentication to support integrity as the e-records are delivered to the agency
  - Hash value change if file was tampering

Citations

- No revision control on the program
- Lack of summary validation reports throughout {program's] lifecycle
- An application program listing was found within the program design binders for the stability application which was not reviewed or approved.
- Failed to validate the MS Excel spreadsheet file (i.e.; lack of audit trail functions for the spreadsheet file, failure to create and maintain specifications for the spreadsheet file)
- Lack of high level functional or structural system diagrams throughout the lifecycle of the program [for all applications]
- Failed to generate or maintain complete software functional or structural design diagrams for all of the applications making up the program throughout the software lifecycle

Citations

- High level specifications for program applications was not a controlled record and it lacked review or approval
- Change control records were not signed off by QC
- No approved protocols defining what tests were to be conducted
- No documented review and approval of test records
- Continued to use a program after a bug was detected
- User screens & user menus did allow for access to view the version of the application
- Failed to document all sites, departments or connections on the network
- User manuals for the software applications obsolete

Citations

- Sharing a username/password with highest level of access amongst several employees
- Failed to produce an approved list of personnel currently authorized to share this username/password.
- Lack of sufficient design control documentation for complete definition of the network (i.e.; high level diagrams identifying all sites / equipment making up the network).
- Electronic records are not reviewed or approved (i.e.; no electronic signatures of review or approval).
- Lack of definition documentation and security for a database
- Lack of review or approval by the QCU of LAN wiring diagram, which is not a controlled record…

Citations

- Failed to generate or maintain complete documentation of the myriad (>100) of user interface displays that have been developed and maintained by company personnel for the system
- Process Control System Security SOP does not adequately describe all the steps performed for security and computer access
- No written procedure to describe the process used to assign, maintain passwords and access levels to the system
- Nonviable particle measurements
  - recorded floppy disk and data manually transferred to data base system
  - No formal evaluation to confirm that the measurements…printed…is an accurate reflection of the data
  - When the diskette is filled, the original data is not retained and is overwritten and/or deleted
  - No established written SOP to describe reuse of the 3.5” floppy disks.
- SOP was not followed for establishment of validation requirements for GMP computer systems

483s

- North American Science Associates - Nov 1998
  - failure to maintain adequate controls over computers & systems…no current listing of individuals who have access, no audit trail
- Hydro Med Sciences - Feb 1999
  - computer software programs have not been validated
  - programs do not secure files from data loss
  - analysts can delete whole data files
  - no security SOPs or back-up
- Fairbanks Memorial - Apr 1999
  - failure to control computer or related systems
  - publicly posted employee user name and computer password
  - terminated employees still had access
  - No change control records
- Linweld - Aug 1999
  - failure to maintain a computer system with validated program capabilities
  - no testing of system after installation
  - validation protocol incomplete
  - protocol execution pre-dates protocol and requirements approval
  - lack of change control procedure

483s

- Hoffman-LaRoche - Dec 1999
  - Lab computer system software
- Intersurgical - May 2000
  - failure to validate computer software
- Baxter Healthcare - Aug 2000
  - … electronic cGMP records into conformance
- Pharmacia - Jan 2001 (2 sites)
  - network program lacked adequate validation
- Zeus - Mar 2001
  - firm failed to validate the electronic documentation system
- Stough Enterprises - April 2001
  - failure to establish and implement adequate computer security

483s

- Meridien Bioscience - June 2001
  - database has not been validated nor does it include necessary controls
- Michigan Instruments - Oct 2001
  - no documentation to show electronic records meet requirements
- Luneau SA - Oct 2001
  - Failure to validate computer software for its intended
- Earlham College
  - Laboratory using an electronic record system for processing and storage of data from the AA and HPLC instruments
  - Not set up to control the security and data integrity
  - Not password controlled
  - No systematic back-up provision
  - No audit trail of the system capabilities
  - Not appear to be designed and controlled in compliance with requirements

Business Stopper!

The computer for disposition control of finished, inprocess and purchased materials, controls and maintains stability sample inventories for commercial and development stability programs, controls stability programs [through test schedules], maintains and manages test results, generates stability study reports for presentation in annual reports, annual product reviews, and New Drug Applications.. is not considered validated because ….

Result v process

Navigate GMP with DBA

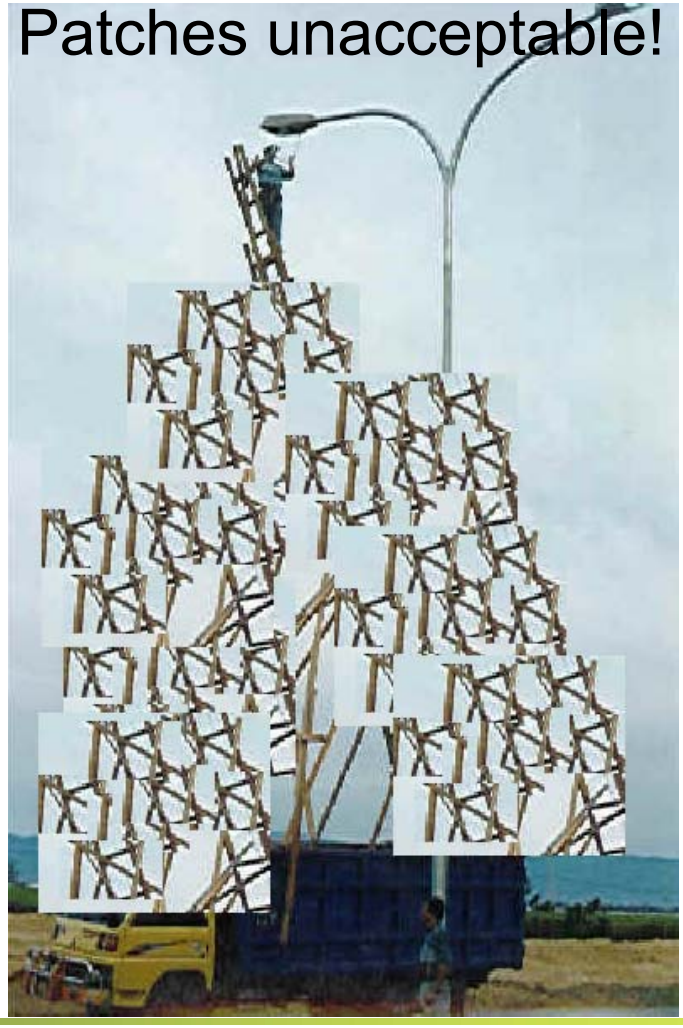
Result OK?

Result v process!

Navigate GMP with DBA

Process unacceptable!

Patches unacceptable!



References

GAMP		www.gamp.org
ISPE		www.ispe.org
PDA	Good Electronic Record Management	www.pda.org
		www.labcompliance.com
		www.21cfrpart11.com
FDA		www.fda.gov

groups.yahoo.com/group/21cfrpart11/messages/

Questions?