

컴퓨터 밸리데이션

식품의약품안전청
의약품품질과

관리체계 탄생

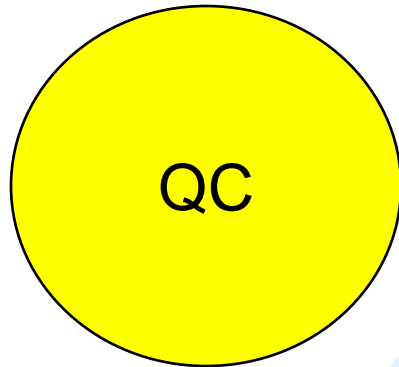
해상

화재

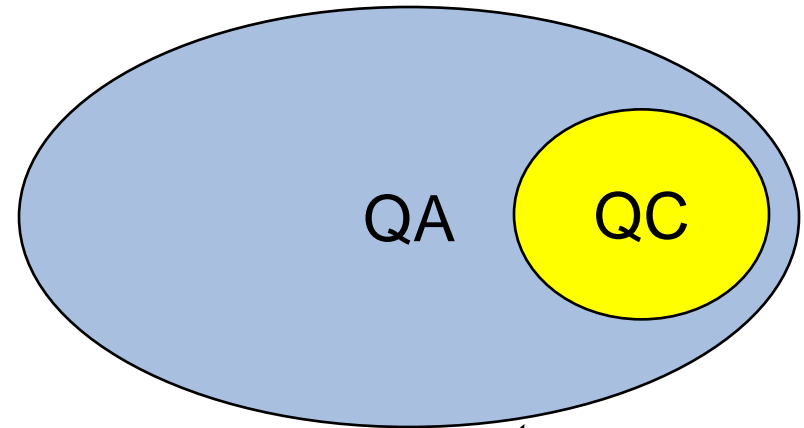
자동차

생명

?

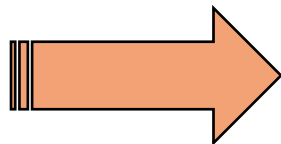


자동화



문제점

역사



문제점

군사시설
(핵시설)

금융거래
(은행, 증권)

사회시설
(교통, 발전소)

의약품
(안전성)

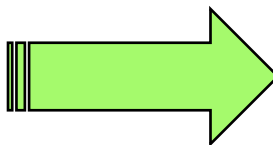
보안성
자료신뢰성



속도(리콜, 통계, 분석)



임상
제조
유통



Business + GMP

정확성

신뢰성

완전성

표 2

Trend



Annex1

Annex3

Annex6

Annex11

?

色

相

形

效

結

기초학문

해부학

생리학

병리학

약리학



Function

Structure

6.6 컴퓨터시스템 밸리데이션

컴퓨터시스템의 자료를 정확하게 분석 · 관리 · 기록하고
미리 정하여진 기준에 맞게 자료를 처리한다는 것을 고도의
보증수준으로 검증하고 문서화하는 밸리데이션으로서
기계 · 설비 · 시스템별로 실시하여야 한다.

제8조(컴퓨터시스템 밸리데이션 방법 등)

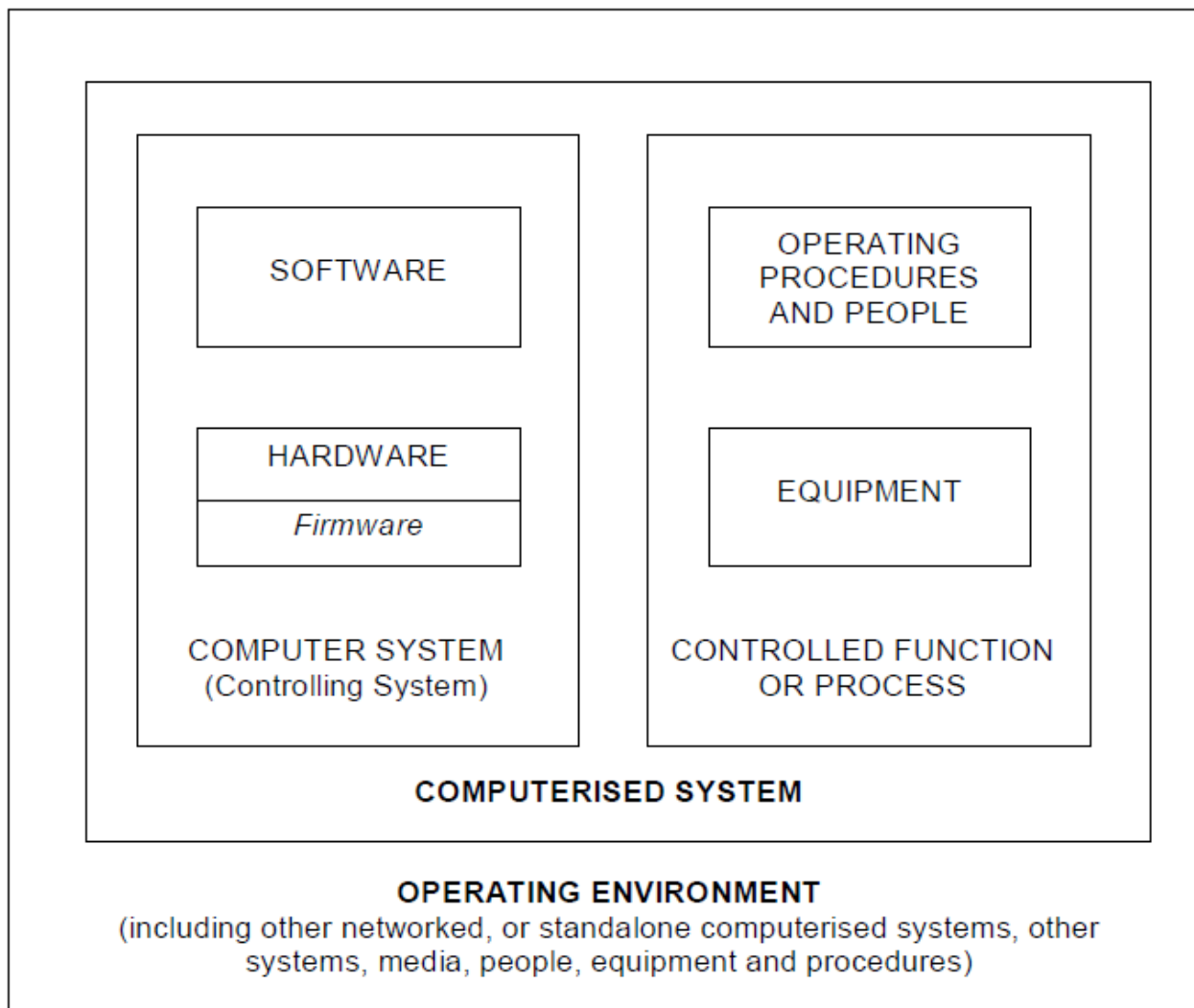
- ① 컴퓨터시스템 공급자, 컴퓨터 및 관련 장비에 대하여 평가하여야 한다. 다만, 공급자 평가가 불가능한 경우 생략할 수 있다.
- ② 시스템 설치가 완료된 후에는 제3조에 따른 적격성평가를 실시하여야 하며 시스템에 따라 적격성평가의 범위를 결정하여야 한다.
- ③ 시스템 규격(System Specification) 및 기능 규격(Functional Specification)에 대하여 밸리데이션 하여야 한다.
- ④ 컴퓨터시스템 밸리데이션에는 변경관리, 유지·보수, 교정, 보안성 및 작업원에 대한 교육 등이 포함되어야 한다.

Computer System

- Computer hardware components assembled to perform in conjunction with a set of software programs, which are collectively designed to perform a specific function or group of functions.

Computerised System

- A computer system plus the controlled function that it operates.



Functional Testing

A process for verifying that software, a system, or a system component performs its intended functions.

Functional Specifications

Statements of how the computerised system will satisfy functional requirements of the computer-related system.

System Specifications

Describe how the system will meet the functional requirements.



Principle

- Computerised system **replaces a manual operation**, there should be **no resultant decrease in product quality or quality assurance**
- Consideration should be given to the risk of losing aspects of the previous system which could result from reducing the involvement of operators.



Personnel

1. It is essential that there is the closest co-operation between key personnel and those involved with computer systems. Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilises computers. This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerised system.

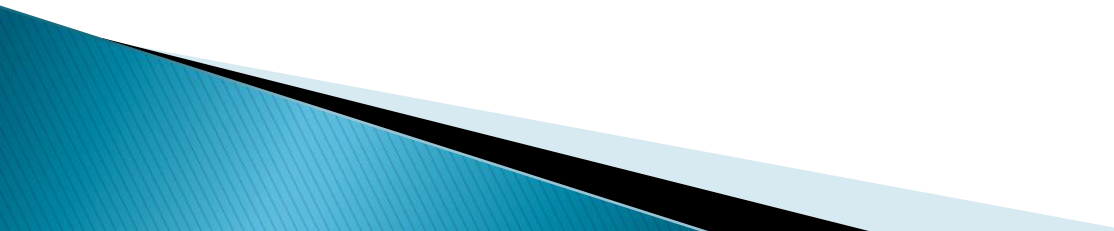
Validation

2. The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether or not novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying.

System

3. Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.

System

4. A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.
- 

System

5. The software is a critical component of a computerised system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.

System

6. The system should include, where appropriate, built-in checks of the correct entry and processing of data.

System

7. Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as a part of this testing and validation.

System

8. Data should only be entered or amended by persons authorised to do so. Suitable methods of deterring unauthorised entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alteration of authorisation to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorised persons.

System

9. When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.



System

10. The system should record the identity of operators entering or confirming critical data. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (an "audit trail").

System

11. Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. **Every significant modification should be validated.**

System

12. For quality auditing purposes, it should be possible to obtain clear printed copies of electronically stored data.

System

13. Data should be secured by physical or electronic means against wilful or accidental damage, in accordance with item 4.9 of the Guide. Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used.

System

14. Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.

System

15. There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them.

For example, information required to effect a recall must be available at short notice.



System

16. The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.

System

17. A procedure should be established to record and analyse errors and to enable corrective action to be taken.(병리/약리)

System

18. When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency

System

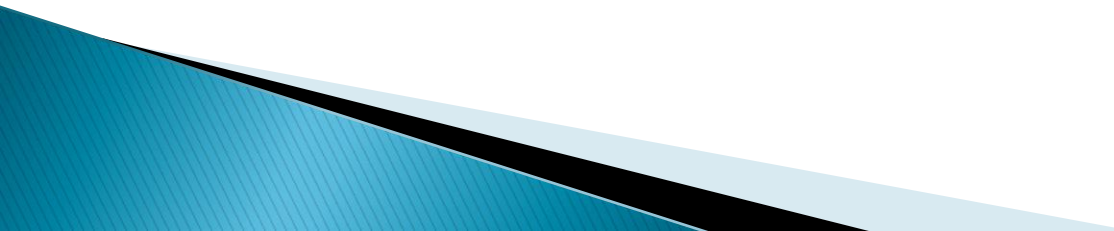
19. When the release of batches for sale or supply is carried out using a computerised system, the system should allow for only a Qualified Person to release the batches and it should clearly identify and record the person releasing the batches.

Q1

컴퓨터시스템 밸리데이션 관련자료가 있는지

- 관련자료는 약사법시행규칙 [별표 2] 및 의약품등 밸리데이션 실시
에 관한 규정(식약청고시) 및 새 GMP 해설서(제4개정) 등이 있음
- 외국의 관련규정은 FDA CFR Sec. 211.68의 Automatic,
mechanical, and electronic equipment, ICH Q7의 5.4 Computerized
Systems, WHO의 Validation of Computerized Systems, EU의
Computerized Systems 등이 있으니 참고하시기 바랍니다

REFERENCES FOR RELEVANT STANDARDS AND GMP GUIDES / CODES

- (1) EU Annex 11 to the EU guidelines of Good Manufacturing Practice for Medicinal Products.
 - (2) Annex 11 to PIC/S Guide to Good Manufacturing Practice for Medicinal Products, Document PH 1/97 (Rev. 3), PIC/S Secretariat, 9-11 rue de Varembe, CH-1211 Geneva 20
 - (3) GAMP Guide for Validation of Automated Systems, GAMP4 (ISPE (GAMP Forum), 2001)
 - (4) Australian Code of GMP for Medicinal Products, August 2002.
 - (5) WHO Guideline for GMP for Manufacture of Pharmaceutical Products.
- 

REFERENCES FOR RELEVANT STANDARDS AND GMP GUIDES / CODES

(6) Relevant CFR sections of the USFDA Register:

Hardware

21 CFR 211.63,
67, 68

21 CFR Part 11

Electronic Records: Electronic Signatures

Software

21 CFR 211.68,
180, 188, 192

21 CFR Part 11

Electronic Records: Electronic Signatures

Quality System

21 CFR 820

Quality system regulation

GLP

21 CFR 58

Good laboratory practice for non-clinical laboratory studies

(7) ISO standards:

Quality management and quality assurance

ISO 9000-1 Part 1: Guidelines for selection and use.

ISO 9000-3 Part 3: Guidelines for the application of ISO9001:1994 to the development, supply, installation and maintenance of computer software. See also current Tick-IT Guide for construction, software engineering, assessment and certification (see ref. 12 re:BSI DISC London)

Quality Management and quality system elements

ISO 9004-1 Part 1: Guidelines.

ISO 9004-2 Part 2: Guidelines for Services .

ISO 9004-4 Part 4: Guidelines for quality improvement.

ISO 10005: 1995 Quality management - Guidelines for quality plans.

ISO 10007: 1995 Quality management - Guidelines for Configuration Management

REFERENCES FOR RELEVANT STANDARDS AND GMP GUIDES / CODES

Life cycle management

- ISO/IEC 12207:1995 Information Technology - Software Life Cycle processes
- ISO/IEC 17799:2000 (BS 7799-1:2000) Information technology – Code of practice for information security management.

(8) IEEE Publications:

IEEE 729	Glossary of Software Engineering Terminology
IEEE 730	Quality Assurance Plan
IEEE 828	Software Configuration Management Plans
IEEE 829	Software Test Documentation
IEEE 830	Guide to Software Requirements Specification
IEEE 983	Guide to Software Quality Assurance Planning
IEEE 1012	Software Verification Plans
IEEE 1298	Software Quality Management System Part 1: Requirements

(9) British Standards:

BS 7799: 1999 "Information Security Management", BSI DISC 389
Chiswick High Road, London W4 4AL
(Tel:+44 181 995 7799 Fax:+44 181 996 6411
<http://www.bsi.org.uk/disc>)

BS 7799: 2000 Information technology – Code of practice for
information management

(10) DISC BSI Guides

DISC PD 5000 series of 'Codes for Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence' (including DISC PD 0008:1999 in Pt 1):

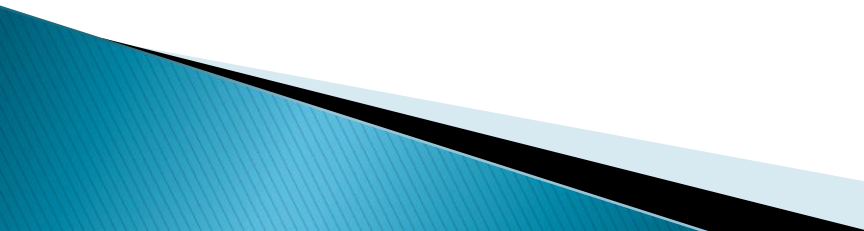
Pt 1	Information Stored Electronically
Pt 2	Electronic Communication and e-mail policy
Pt 3	Identity Signature and Copyright
Pt 4	Using Certification Authorities
Pt 5	Using trusted Third Party Archives

DISC PD 3002	Guide to BS 7799 Risk Assessment and Risk Management (ISBN 0 580 29551 6)
DISC PD 3005	Guide on the selection of BS 7799 controls (ISBN 0 580 33011 7)

- (11) 'Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application', US Dept. of Health and Human Services and all FDA Centers/ Offices, February 2003. (<\\CDS029\CDERGUID\5505dft.doc>) – draft guidance for comment.

SUGGESTED FURTHER READING

1. Good Computer Validation Practices – Common Sense Implementation [Stokes, Branning, Chapman, Hambloch & Trill. Interpharm Press, USA: ISBN: 0-935184-55-4]
2. Computer Systems Validation for the Pharmaceutical and Medical Device Industries [Chamberlain. ISBN 0-9631489-0-8].
3. Validating Automated Manufacturing and Laboratory Applications, [Wingate et al., Interpharm Press, USA: ISBN 1-57491-037-X]
4. Validation of Computerized Analytical Systems, Interpharm Press, L. Huber, ISBN: 0-935184-75-9, 1995
5. General Principles of Software Validation - Final Guidance for Industry and FDA Staff (FDA, CDRH, January 2002)

6. PDA Technical Report No 18, "Validation of Computer-Related Systems", PDA Journal of Pharmaceutical Science and Technology, 1995 Supplement, Vol. 49, No.S1
 7. PDA Technical Report No. 32, "Report on the Auditing of Suppliers providing Computer Products and Services for Regulated Pharmaceutical Operations" (PDA, 1999)
 8. 'Validation of Process Control Systems: a Guideline by GMA & NAMUR', in Section 5 of GAMP-3 (1998) Vol. 2, Best Practice for Users and Suppliers.
 9. PDA Technical Report No. 31: "Validation and Qualification of Computerised Laboratory Data Acquisition Systems", PDA Journal of Pharmaceutical Science and Technology, 1999 Supplement, Vol. 53, No.4
 10. Guidance for Industry - 'Computerized systems used in Clinical Trials', US FDA, April 1999
- 

11. GLP Consensus Document 'The Application of the Principles of GLP to Computerised Systems', 1995, OECD/ OCDE/GD (95) 115 (Environment Monograph No.116)
12. Computer Systems Validation in Clinical Research, 1997, ACDM/ PSI Working Party. (ACDM, PO Box 129, Macclesfield, Cheshire SK11 8FG England)
13. ICH Topic E6: 'Guideline for Good Clinical Practice'. (ICH-GCP/CPMP/ICH/135/95)
14. EU GMP Guide Annex 15, 'Qualification and Validation', European Commission, July 2001, (based on PIC/S recommendations)
15. APV Guidance, Appendix 9 to GAMP4 'Guide for Validation of Automated Systems', ISPE (GAMP Forum), 2001

Q2

컴퓨터 시스템 밸리데이션은 언제까지 모두 마쳐야하는지

- 컴퓨터시스템 밸리데이션은 컴퓨터시스템 공급자, 컴퓨터 및 관련 장비에 대하여 평가하는 것으로 컴퓨터시스템을 이용하여 의약품 제조하는 경우 '10.1.1 이후 밸리데이션된 컴퓨터시스템을 이용하여 의약품을 제조하여야 함

Q3

측정된 결과가 중앙데이터시스템으로 송부·저장되는 제조용수 배관에 설치된 각각의 수질계측기에 대해 컴퓨터시스템 밸리데이션을 실시해야하는지

- 컴퓨터시스템 밸리데이션 적용범위는 설치된 시스템이 의약품의 품질에 얼마나 영향을 주는가에 따라 달라질 수 있으며, 단순 정보용 등의 경우에는 밸리데이션 대상에 해당하지 않음
- 따라서, 해당 시스템의 명확한 사용목적에 따라 밸리데이션 실시여부를 결정하는 것이 타당할 것으로 사료됨
- 다만, 상기의 수질계측기가 의약품의 품질에 직·간접적으로 영향을 미치는 정보를 기록, 전송, 표시, 처리, 평가, 출력, 기록 또는 저장하는 컴퓨터시스템이라면 밸리데이션을 실시하는 것이 바람직할 것으로 사료됨

Q4

컴퓨터 시스템 밸리데이션 실시 전 반드시 URS, FS, FAT, SAT 및 공급자에 대한 평가를 실시해야하는지, 오래전 구입하여 URS, FS, FAT, SAT를 실시 할 수 없다면 생략이 가능한지

- 의약품등 밸리데이션 실시에 관한 규정 제8조제1항에 따라 공급자 평가가 불가능한 경우 기설치된 컴퓨터 시스템의 URS, FS, FAT, SAT 등을 생략할 수 있으며, 동 규정 제3조제6항제1호의 규정에 따라 기 설치된 컴퓨터 시스템의 경우 일부 적격성평가를 생략할 수 있음

Q5

HPLC 및 GC 같은 기기는 컴퓨터시스템 밸리데이션 대상인지

- HPLC 및 GC가 기준 및 시험방법과 관련된 컴퓨터시스템과 연결되어 있는 경우 시스템규격과 기능규격에 대하여 밸리데이션을 실시하여야 하며, 또한 변경관리, 유지·보수, 교정, 보안성 및 작업원 교육 등을 포함하여야 할 것으로 사료됨

INSPECTORS - PREPARING FOR AN INSPECTION	
1.	Details of the organisation and management of IT/Computer Services and Project Engineering on Site.
2.	The regulated user's policies on procurement of hardware, software and systems for use in GxP areas.
3.	The regulated user's policy on the validation of GxP computerised systems
4.	A list of IT/Computer Services Standards and SOPs.
5.	The project management standards and procedures that have been applied to the development of the various applications.
6.	Identify work contracted out routinely for systems support and maintenance.
7.	A list, or inventory, of all Computerised Systems on site by name and application for business, management, information and automation levels. The list should also indicate validation status and risk ranking. (Include basic schematics of installed hardware and networks).
8.	Identify and list those systems, sub-systems, modules and/or programs that are relevant to GxP and product quality. Cross-refer to the lists provided for '6' above.
9.	For the GxP significant elements and systems identified in '7' please provide additional information as below:
10.	Details of disaster-recovery, back up, change-controls, information security, and configuration management.

11.	A summary of documentation that generally exists to provide up-to-date descriptions of the systems and to show physical arrangements, data flows, interactions with other systems and life cycle and validation records. The summary should indicate whether all of these systems have been fully documented and validated and confirm the existence of controlled system description documents as required by EU GMP A11 (4).
12.	A statement on the qualifications and training background of personnel engaged in design, coding, testing, validation, installation and operation of computerised systems, including consultants and sub-contractors, (specifications, job descriptions, training logs).
13.	State the firm's approach to assessing potential suppliers of hardware, software and systems.
14.	Specify how the firm determines whether purchased or "in-house" software has been produced in accordance with a system of QA and how validation work is undertaken.
15.	Document the approach that is taken to the validation and documentation of older systems where original records are inadequate.
16.	Summarise the significant computer system changes made since the last inspection and plans for future developments.
17.	Ensure that records relating to the various systems are readily available, well organised, and key staff are prepared to present, discuss and review the detail, as necessary.

Software Related - Inspector's Aide Memoir³³

Life Cycle Stage	Project Stage Activity	Evidence for Review
1. Development	Develop URS/FS/DS	URS/FS/DS Documents
1. Development	Plan Testing	Test plan and test scripts
1. Development	Plan documentation of Testing	Written document describing how testing should be documented.
2. Implementing	Select programming language and tools	Document recording programming choices
2. Implementing	Write/create software program.	Documented source code with comments; explanation of function; in-data and expected out-data for each structured module. How modules influence each other. If program is purchased, how is access to source code guaranteed? ⁵⁶

3. Testing (Modules)	Make sure each module only accepts allowed in-data and gives only allowed out-data. Testing should discover incorrect data and logic errors.	Sample reports from testing if possible. Has testing covered boundaries of limits and also the input of invalid data? Have all tests been documented? Have all errors/failures been followed up?
Testing (Integrated Modules).	Same type of tests but applied after integrating the modules.	Same kind of review of evidence. If the program is purchased, then validation proof needs to have been assessed by regulated user.
4. Maintenance	Correct errors, update versions when needed.	Formal routines and records for configuration management and change control. Regression testing and periodic evaluation (as a system goes through multiple changes over time)
5. Documentation	System documentation (including software) correct and updated.	User handbook, supporting SOPs, correct versions.

6. Re-validation.	Re-validate when changes are made to the program.	Changes are reviewed and decisions documented. Routines and records are in-place, scoped dependent on the size/complexity of the changes
7. Other matters	Alternative routines are put in place for system failure and training includes this.	The alternative routines are documented, including training records.

Computer System Validation Related – Inspector's Aide Memoir

Number	Element	Control Measure Checks
1.	Define	Is the system defined? What should it do? Is there a written validation plan? Are there full specifications? Are there written protocols? (Including acceptance criteria).
2.	Testing	Do the test records show that 'in' and 'out' data meets the specifications?
3.	Documented results	Are the results complete and documented?
4.	Verify correctness	Are data and documentation correct and complete? Have these been verified by the regulated user?
5.	Compare with Acceptance Criteria	Have competent responsible personnel carried out the validation and review work? Is this all documented?
6.	Conclusions	Are conclusions complete, meaningful and based on results? Are acceptance criteria fulfilled? Are there any conditional conclusions?
7.	Approval	Has approval been formally recorded? Was there any QA/QC involvement at the regulated user?
8.	On-going evaluation	What is the procedure to ensure on-going evaluation of the system? What are the change control procedures?

Annex 11 – Inspector's Checklist

Point	Requirement	Inspector's Check/Comment
Personnel (1)	Key personnel/computer specialists co-operate.	
Personnel (1)	Project and user personnel are trained and any necessary experts are involved.	
Validation (2)	Life-cycle model; formal policy and procedures in place.	

System (3)	Influence of environment	
(4)	There is a written, up to date, detailed description of the system.	
(5)	Software has been produced according to a quality assured system.	
(6)	Checks of data and calculations built in.	
(7)	System tested and validated. Verified against previous/or manual system being replaced.	
(8)	Data entry and change only by authorised personnel. Password / security management.	
(9)	Critical data (GXP data) verified by a 2 nd person, or by a validated electronic method.	
(10)	Audit trail for data entry and processing.	

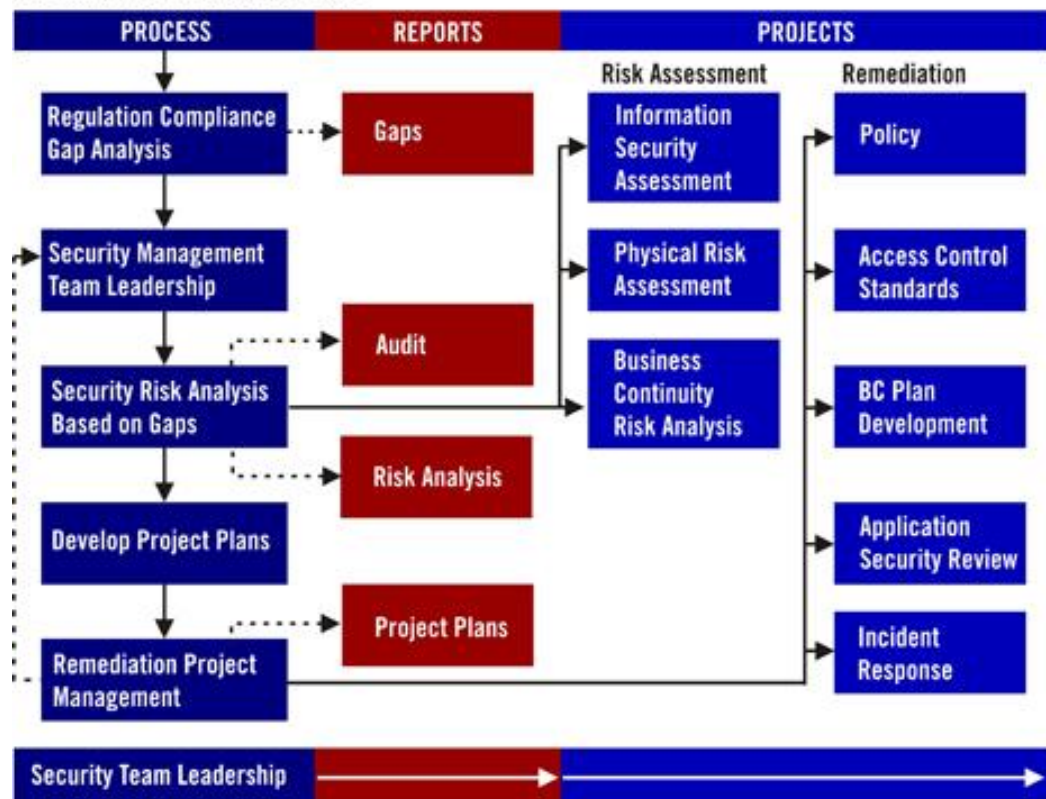
Information Security Risk Management for ISO27001 / ISO17799

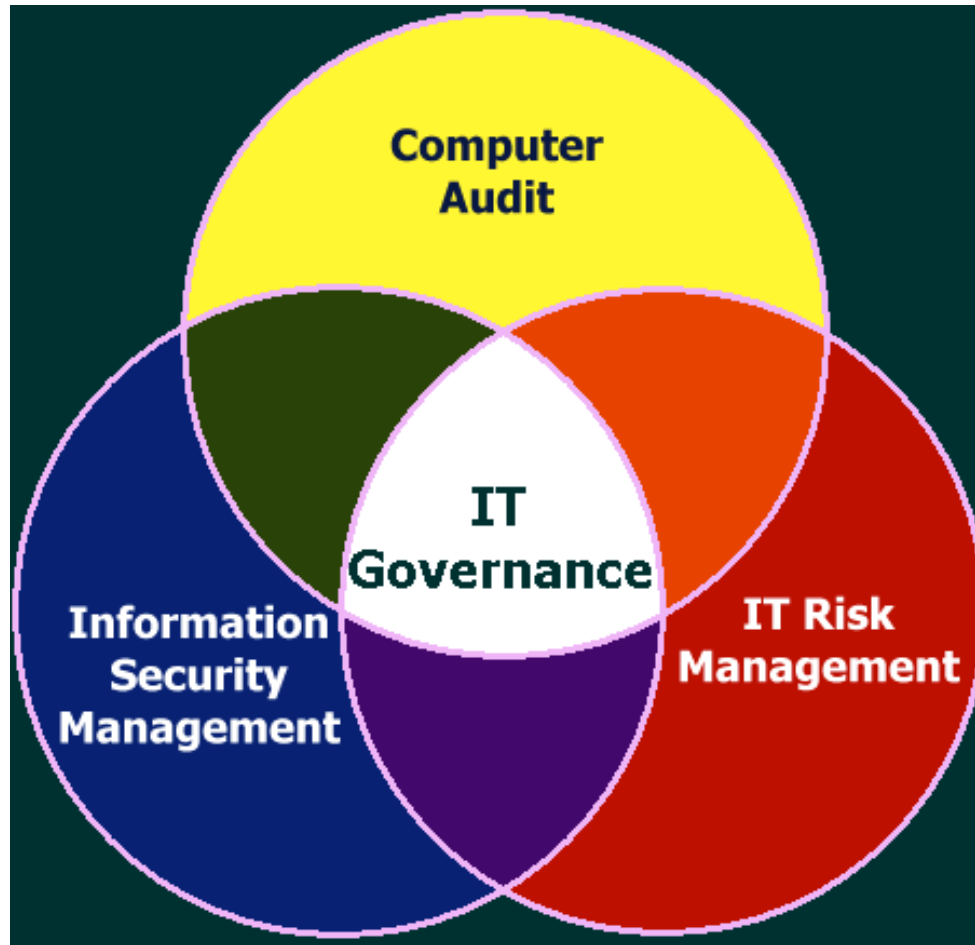
Alan Calder
Steve G Watkins



IT Governance Publishing

INFORMATION SECURITY PROGRAM







Analog vs Digital

