EUROPEAN COURT OF AUDITORS

AUDIT METHODOLOGY AND SUPPORT

GUIDELINE FOR
AUDIT OF IT ENVIRONMENT

CONTENTS

For further information please contact:
European Court of Auditors - CEAD Chamber
Audit Methodology and Support - IT audit team
E-mail: ams.contact@eca.europa.eu

ECA - 2011

1 INTRODUCTION

Information technology

1. The resources used in information technology (IT) are infrastructure, applications, information and people. An IT system designed for use in financial and management reporting will have procedures and databases for initiating, recording, processing and reporting transactions (as well as events and conditions) and maintaining accountability for the corresponding assets, liabilities and equity.

2. Increasingly, the use of IT systems is having an impact on audit. The risks associated with IT must be taken into account when evaluating the reliability of accounts, the legality and regularity of underlying transactions and the effectiveness of internal control systems.

Scope of this guideline

3. The methodology for auditing in an IT environment varies according to whether the objective is a financial, performance or IT audit. For illustrative purposes, this guideline focuses on the task of financial audit in an IT environment in accordance with the Court's Audit Policies and Standards (CAPS).

4. Section 2 of the guideline presents the risks introduced by computerised information systems and the interconnections between financial audit and the IT environment.

5. Section 3 provides step-by-step guidance for IT audit work in the context of financial audit. It defines eight steps, broken down into planning, execution and reporting phases.

6. Lastly, Section 4 addresses the related procedures arising in the overall context of the Court’s audit work.

7. The guideline concludes with annexes: a "**Checklist for general controls**" and a "**List of application controls**" to help auditors perform IT audit tasks, and an “**IT audit glossary**”.

2 AUDITING IN AN IT ENVIRONMENT

IT risks and controls in the internal control framework

8. Most financial transactions and statements are now processed or produced using IT systems. The procedures for initiating, recording, processing and reporting transactions and recording the corresponding assets and liabilities are usually implemented within IT systems. Given, therefore, that financial data are now predominantly electronic data, financial and administrative controls are also increasingly electronic in nature.

9. The storage and processing of information in IT systems introduces new risks and possible control weaknesses, owing mostly to the ease with which data and the IT systems themselves can be modified.

10. IT systems are one of the five components of the internal control framework *(ISA 315[1], paragraphs A81-A87),* and key IT controls should be in place to mitigate the IT-related risks and thus ensure the confidentiality, availability and integrity of data and the efficiency and effectiveness of business processes. The following table gives examples of risks and their IT sources:

Risk	IT-related risk source
Individual errors become systematic	Automation replacing manual operations
Failure to identify the performer of the transaction	Electronic transactions not logged
Unauthorised access and changes to data	Electronic data not properly secured
Loss (destruction) of data	Electronic data not protected (backups and archiving)
Disclosure of confidential information	Electronic data not properly secured
Control weaknesses undetected.	IT risks and controls not (adequately) considered in audit

Table 1: Risks with an IT origin

[1] http://www.ifac.org/sites/default/files/downloads/a017-2010-iaasb-handbook-isa-315.pdf

11. The use of IT systems in business processes changes the nature of audit evidence, the audit trail and the internal control environment. It also creates new vulnerabilities to irregularities and fraud, and new audit procedures are therefore necessary in order to deal with these challenges.

12. Where accounting or other information systems are computerised, the auditor determines whether internal controls are functioning properly to ensure the integrity, reliability and completeness of the data *(INTOSAI Auditing Standards ISSAI 300[2], 3.4).*

Audit objectives

13. The audit of controls on IT systems should have specific objectives, including verification of the accounts or other data produced by the system (e.g. data extracted for sampling purposes). The evaluation of internal controls should vary according to the type of audit and the degree of reliance the auditor wishes to place on them *(INTOSAI Auditing Standards ISSAI 300, 3.2).*

Reliability of data

14. When IT systems data are an important part of the audit and data reliability is crucial to accomplishing the audit objective, auditors need to satisfy themselves that the data are reliable and relevant (*INTOSAI Auditing Standards ISSAI 300, 5.2*).

15. Data produced, stored or provided to the auditor by means of IT should not be treated as reliable until the auditor has convincing evidence that this is so. ***The components of reliability are accuracy, completeness and validity*.** The quality of the data received from the auditee may significantly influence whether or not the audit objectives are achieved.

16. Evidence for the reliability of the computerised data provided by an auditee may come, depending on the nature of the data, from assurance that internal controls on IT are functioning securely and correctly, from cross-checking of the data (e.g. by reconciling them with data from other sources), or from a combination of the two.

17. The absence of appropriate IT controls may give rise to conditions and events indicating a risk of material misstatement. This in turn would influence the nature, timing and extent of subsequent IT-related audit procedures.

[2] http://www.issai.org/media(631,1033)/ISSAI_300_E.pdf

Use of IT audit in financial audit

18. The objectives of IT audit in the context of a financial audit include:

a) Understanding the overall impact of IT on key business processes;

b) Assessing management controls on IT processes;

c) Understanding how the use of IT for processing, storing and communicating information affects internal control systems, inherent risk and control risk;

d) Evaluating the effectiveness of controls on IT processes which affect the processing of information.

Use of IT audit in performance audit

19. IT audit may be used in the context of a performance audit when:

a) The audit focuses on the performance of IT systems;

b) The audit examines the efficiency and effectiveness of a business process and/or programme where IT is a critical tool for the organisation managing these processes or programmes;

c) Data reliability is to be assessed.

Typical IT audit work in the Court

20. IT audit work in the Court occurs mainly in the context of:

a) Financial audits: reviewing key general controls and related application controls on information systems;

b) Compliance audits: reviewing whether IT controls comply with rules and regulations, usually the Financial Regulation[3] (FR) and Internal Control Standards[4] (ICS);

c) Specific IT audits: when the main audit objective is linked to the effectiveness and efficiency of IT.

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002R1605:20071227:EN:PDF

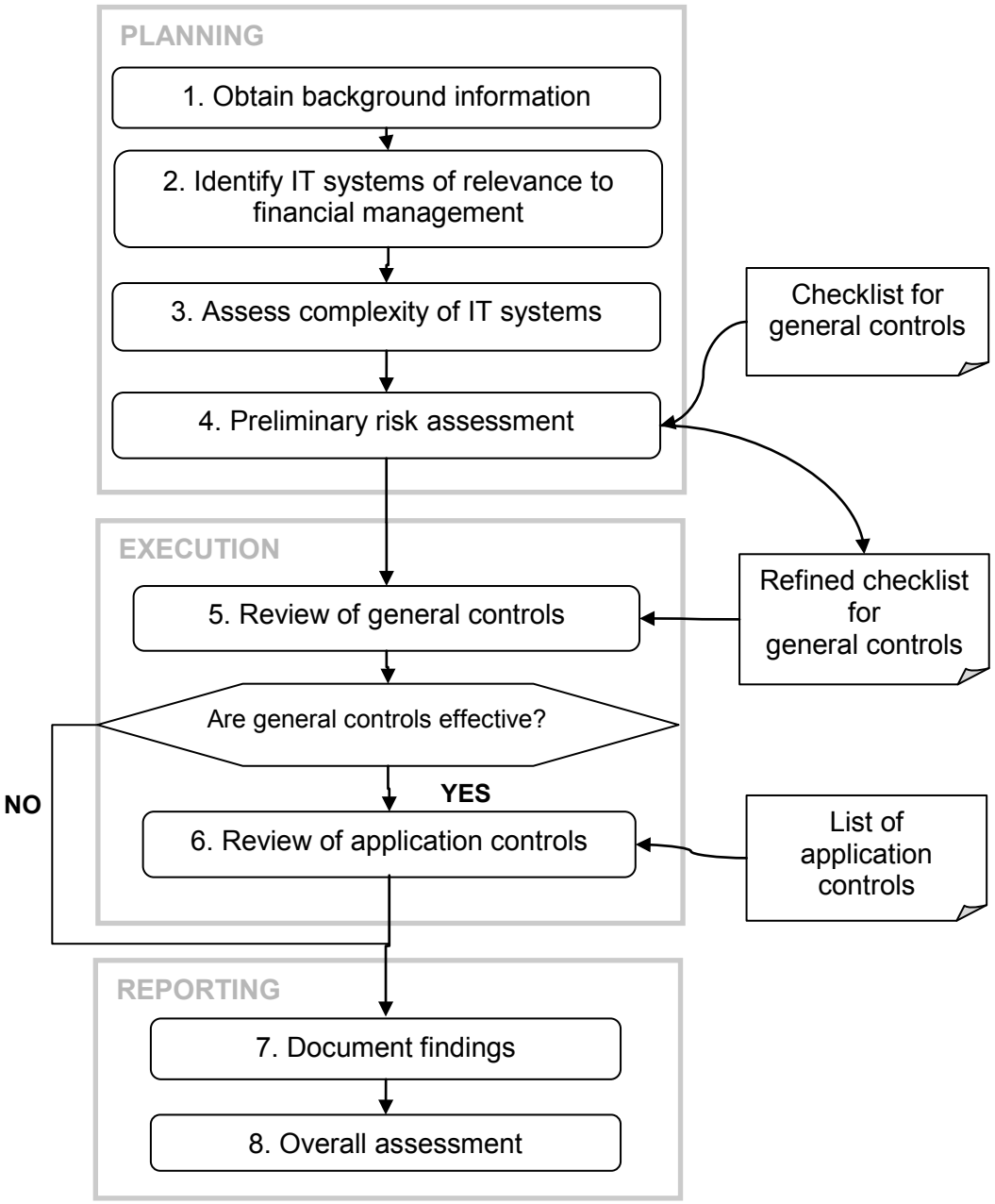
4 http://ec.europa.eu/budget/library/biblio/documents/control/sec_2007_1341_annexes_en.pdf

3 IT AUDIT APPROACH

IT audit tasks

21. The following IT audit tasks are necessary so that audits can be planned and implemented fully in accordance with the CAPS.

22. IT audit work consists of the following steps:



3.1 *Planning phase*

23. The objective of the planning phase is to identify risks that are relevant to the audit goals and determine which controls will be assessed during the execution phase:

a) **General controls** (as for the IT control environment);

b) **Application controls** (in IT applications of relevance to financial management).

Step 1. Obtain background information

24. During the planning phase it is important for the auditor to obtain an understanding of the auditee's IT systems, an inventory of the auditee's IT systems and resources (IT budget and staffing, IT organisation, software and hardware) and a statement of the concerns arising from previous internal or external audits of IT systems.

Step 2. Identify IT systems of relevance to financial management

25. IT systems for accounting and financial reporting comprise procedures and databases for initiating, recording, processing and reporting transactions and recording the auditee's corresponding assets and liabilities.

26. The auditor must identify which IT applications are important in the context of financial reporting and business management and obtain sufficient information and understanding in their regard.

27. In order to facilitate the evaluation of risks and the planning of IT audit tasks, the auditor should document:

a) which IT applications feed into the financial statements;

b) which transactions are processed through these IT applications;

c) which areas of accounts (such as administrative expenditure) are covered by these IT applications.

Step 3. Assess the complexity of the IT systems

28. The purpose of assessing the complexity of IT systems is to:

a) Identify risks - complex systems are more risky than simple ones;

b) Decide whether there is a need for external assistance. In principle, auditors are competent to carry out IT audit tasks in relation to simple systems, with the IT audit team providing support in the audit of more complex systems.

29. The following factors will influence this assessment:

a) Hardware and network complexity;
b) IT applications and data entry methods;
c) IT organisation;
d) The presence of systems under development or recently subject to change;
e) The sensitivity of the processed data;
f) Any specific difficulties affecting the audit trail;
g) The auditor's technical knowledge and skills.

Step 4. Preliminary risk assessment

30. Using all the information obtained in the previous steps, the auditor will then make a preliminary risk assessment.

31. Just as in the more general audit context, internal control in IT comprises two elements:

a) the **internal control environment,** i.e. the overall attitude**,** awareness and actions of management;
b) **internal control procedures,** i.e. procedures complementary to the control environment which contribute to the entity's achievement of its objectives.

32. Please note that the **overall assessment of control risk should not be better to the assessment of the internal control environment**, since even excellent control procedures can be undermined by a poor control environment.

Identifying the risk of material misstatement

33. The auditor should be aware of conditions or events that may indicate a risk of material misstatement consequent upon the use of IT *(ISA 315, paragraphs A33 and A115 and Appendix 2).* The following is a non-exhaustive list of factors that should be considered, when performing the preliminary risk assessment, as contributing to the risk of material misstatement:

a) Changes in the IT environment;
b) Installation of significant new IT systems;
c) Insufficient controls on the transfer of data between IT systems;
d) Inconsistency between the entity's IT and business strategies.

Output of the risk assessment

34. The auditor should:

a) **Refine the checklist for general controls** (see annexes), which summarises the risks that are customarily encountered at the Court's auditees (EC and Agencies). Such risks relate mostly to the integrity and confidentiality of data;

b) **Decide** whether or not to include application controls during the execution phase.

35. Application controls on robust IT systems (e.g. ABAC and SAP at the Commission) should be reviewed when auditing the owner of the system rather than other users (Agencies, joint undertakings, etc.).

Planning of IT audit work

36. The results of the planning phase (steps 1-4) should be stated in the corresponding APM.

3.2 *Execution phase*

What are general controls?

37. General controls relate to the environment within which automated application systems are developed, maintained and operated. They are concerned with IT-related policies, procedures and working practices *(ISA 315, Appendix 1).*

38. They are used to ensure the proper development, implementation and maintenance of all automated applications and the integrity of data files. They therefore minimise risks to the functioning of the organisation's IT systems and infrastructure and specific risks to applications.

39. **General controls** include:

a) *IT governance and management controls:* These are high-level controls designed to provide a formal IT governance framework aligned with the business strategy. IT strategic planning and monitoring, IT policies and procedures, IT roles and responsibilities, the segregation of duties, IT risk, project and investment management, and legal and regulatory compliance can all be considered IT governance and management controls;

b) *Data management controls* ensure that data are properly stored, archived and disposed of. They also help ensure the reliable production of financial and management information;

c) *Business continuity planning* addresses the scenario of a computer systems breakdown and concerns the organisation’s arrangements for protecting data and continuing or restarting operations in that situation;

d) *Information security controls* help organisations establish and maintain IT security roles, responsibilities, policies, standards and procedures. They include logical access controls aimed at ensuring that data can only be seen or altered by authorised persons, inside or outside the

organisation, and in accordance with data protection requirements. Information security controls are also concerned with preventing unauthorised access to and interference with IT systems;

e) *Change management controls* provide assurance that systems and controls continue to function as designed;

f) *Outsourcing controls:* Given that more and more organisations now prefer to outsource IT services, it has become crucial to manage service-level agreements. Depending on the scope of outsourcing, inappropriate management could be detrimental to the IT areas subject to control.

Step 5. Review of general controls

40. The most important criterion for the information when reviewing general controls in financial audit is **integrity(reliability),** which relates to audit assurance that the information is valid, accurate and complete. In a performance audit, the most important aspects may be efficiency and effectiveness.

41. The effectiveness of IT controls will depend on the strength of the general controls. If the auditor concludes that the general controls are effective, he should then assess the effectiveness of application controls. However, ineffective general controls will render application controls ineffective (or severely limit their effectiveness) since they act as a foundation on which specific application controls are built (*ISACA – IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals).* Application controls are to be considered ineffective when, for instance, the necessary logical or physical access controls are not functioning adequately.

42. A **full audit of general controls** can require substantial technical resources. However, adequate assurance can usually be obtained from a more limited examination in the light of the risk assessment performed during the planning phase, and by drawing on other sources of information.

43. The **checklist for general controls** (see annexes) provides guidance for reviewing general controls through a set of close-ended questions that are mainly concerned with the most significant control objectives in relation to data reliability and the IT control environment. The checklist will help auditors check the main IT control objectives, which are based on the COBIT framework in reference to the EU's regulatory framework and information criteria.

44. Auditors should conduct their examination using the refined **checklist for general controls** that was obtained at the end of the planning phase (see paragraph 34).

45. If the auditor concludes that the general controls are not functioning effectively, the application controls will generally also be ineffective. The auditor should review the application controls only if the general controls are effective (see paragraph 41).

What are application controls?

46. Application controls, which may be **manual** (performed by users) or **automated** (performed by computer software), are procedures that apply to the processing of transactions by individual applications and are designed to ensure the integrity and confidentiality of data.

47. Application controls relate to procedures that are used to initiate, record, process or report transactions or other financial data. They help ensure that transactions were duly authorised and completely and accurately recorded and processed *(ISA 315, paragraph A97).*

48. The main objectives of application controls are:

a) *Completeness* – the application processes all transactions, and the resulting information is complete;

b) *Accuracy* – all transactions are processed accurately and as intended, and the resulting information is accurate;

c) *Validity* – only valid transactions are processed, and the resulting information is valid.

d) *Authorisation* – only duly authorised transactions are processed;

e) *Segregation of duties* – the application provides for and supports appropriate segregation of duties and responsibilities as defined by management.

49. These objectives are targeted using six main types of application control (COBIT):

a) System documentation controls;

b) Input controls;

c) Processing controls;

d) Output controls;

e) Data transmission controls;

f) Standing data and master file controls.

Step 6. Review of application controls

50. Application controls on systems should be audited in accordance with the risk assessment performed during the planning phase, focusing on systems which have a direct impact on financial data and are more material to the audit objective. For instance, compared with an accounting application, a document management system may have only an indirect impact on financial data.

Manual and automated application controls

51. Automated application controls which are embedded in an application reduce the risk of human error or manipulation of information and are therefore more reliable than manual controls. Once properly established, automated application controls are reliable until the next change to the program takes place. Efficient general controls will lead to more reliance on automated rather than manual application controls.

52. Where manual application controls are in place, the auditor should assess arrangements for user cross-checking in the form of a manual comparison of computer-processed data with the source documents.

53. When checking application controls on the systems identified during the planning phase, the auditor may make use of the general framework in the annexed list of application controls.

54. In the case of robust IT systems (e.g. ABAC, SAP), the auditor should identify other application controls in accordance with the financial regulatory framework after evaluating the complexity of the application and the related IT risks.

55. Remember that application controls on robust IT systems should be reviewed when auditing the owner of the system rather than other users (Agencies, joint undertakings, etc.).

Evidence

56. The auditor may obtain audit evidence by observation, inspection, inquiry and confirmation, reperformance, recalculation, computation, analytical procedures, or other generally accepted methods.

3.3 *Reporting phase*

57. Following the assessment of IT controls the findings should be documented, with a general conclusion on the effectiveness of IT controls, in accordance with the Court's audit methodology.

Step 7. Document findings

58. The auditor should document each significant finding, with a statement of the regulatory framework, facts, conclusion and IT risks.

59. Auditors should explain each control weakness in relation to the IT risks. They should also determine which areas of the accounts could be negatively affected by a control weakness.

Step 8. Overall assessment

60. In addition to the individual findings, the auditors should reach an overall conclusion about IT controls.

61. The assessment may lead to three possible conclusions in the context of the financial audit:

a) IT controls functioned effectively, consistently and continuously during the period under review;

b) weaknesses are noted in the effectiveness and continuity of IT controls, but the overall system is considered reliable;

c) IT controls are unreliable, i.e. they did not function as expected and/or they did not function continuously during the period under review and/or they could not be tested.

Documentation

62. In the same way as any other audit work, IT audit should be executed, documented, supervised, and subject to quality control in accordance with the Court's audit methodology.

4 RELATED PROCEDURES

Need for technical resources

63. The auditor must consider whether the cost of obtaining audit evidence is reasonable. As already stated, adequate assurance can often be obtained from a more limited examination of general controls and by drawing upon other sources of information.

64. The audit of application controls is not necessarily highly technical. Many applications are designed to give definite assurance to management that data and processing are in order, without the need for IT experts. In such cases, the checks and procedures (including manual procedures) routinely carried out by regular users may give satisfactory assurance that data and output are reliable. This level of assurance will also be adequate for auditors – except in the case of **specific IT audits**.

AMS technical assistance

65. The CEAD AMS IT audit team is available to provide auditors with assistance and advice on IT audit-related matters and can participate in carrying out relevant IT tasks in line with the audit objectives. The team can also provide assistance in the following areas:

a) Advice concerning IT controls in the context of preliminary studies and APMs;

b) Evaluation of general and application controls;

c) Specific IT audit tasks;

d) Data collection and analysis.

66. It is recommended that auditors contact the AMS IT audit team in order to clarify and discuss how best to address their IT audit needs.

Need for further technical expertise

67. When technical expertise is necessary for specific IT audit testing tasks (network performance, penetration tests, security issues, user rights, change management, technical documentation, etc.) and the necessary skills and resources are not available in-house, external expertise should be organised to collect the required audit evidence. This assistance should be planned at the preliminary stage of the audit, in coordination with the AMS IT audit team.

Requests for assistance

68. Requests for assistance from the AMS IT audit team should be addressed to the Head of the AMS Unit in CEAD.

5 ANNEXES

5.1 *Checklist for general controls*

It is necessary to assess the IT control environment as a basis for deciding how much audit reliance to place on data produced by computerised IT systems. Weaknesses in the IT control environment have a pervasive impact on all applications and data maintained in that environment.

The following checklist is a set of close-ended questions for use in a limited review of the IT control environment at the audited entity. It will help auditors check the main IT control objectives, which are based on the COBIT framework in reference to the EU's regulatory framework and information criteria, in the following areas:

A. IT governance and management

B. Data management

C. Business continuity planning

D. Information security

E. Change management

F. Outsourcing of IT infrastructure

Activity/entity audited:			
Period/financial year audited:			
Amount of IT budget:			
Number of IT staff:			
Document prepared by (name[s]):		**Date:**	
Document reviewed by (name[s]):		**Date:**	

A. IT GOVERNANCE AND MANAGEMENT CONTROLS

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
1.	***Control objective:*** *IT strategy is aligned with and supports the overall business strategy.* ***References to regulatory framework:*** *FR Arts 28a(2)(a) and 27(3); ICS7* ***Related information criteria:*** *Effectiveness*	PO1.4 PO1.5	1. Is there a multiannual **IT strategy or IT plan** (3-5 years) that is formally approved at an appropriate level? 2. Does the IT strategy have adequate and relevant objectives, budget and performance indicators? 3. Are there IT annual work programmes in line with the IT strategy?		• IT strategy or IT plan • IT annual work programmes
2.	***Control objective:*** *Make effective and efficient IT investments and set and track IT budgets in line with IT strategy and investment decisions.* ***References to regulatory framework:*** *FR Art. 27(3); ICS7* ***Related information criteria:*** *Effectiveness and efficiency*	PO5.3 PO5.4 DS6.3	1. Is IT expenditure planned, managed and monitored within an annual budget which is aligned with the IT strategy and detailed enough to reflect the organisation's priorities?		• IT annual budget (separate or a section of the general budget of the organisation) • Any documents for follow-up of IT annual budget
3.	***Control objective:*** *Provide accurate, understandable and approved policies, procedures and guidelines, embedded in an IT control framework.* ***References to regulatory framework:*** *ICS8 and ICS12* ***Related information criteria:*** *Effectiveness*	PO6.3 PO6.4 PO6.5	1. Are there written and formally approved policies and/or procedures covering most key aspects of IT management: a. Data management and classification? b. Business continuity? c. Information security? d. Risks and controls? e. Change management?		• Policies, procedures, guidelines and manuals

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
4.	***Control objective:*** *Establish transparent, flexible and responsive IT organisational structures and define and implement IT processes equipped with owners, roles and responsibilities.* ***References to regulatory framework:*** *FR Art. 28a(2)(a); ICS3, ICS7 and ICS8.* ***Related information criteria:*** *Effectiveness and efficiency*	PO4.1 PO4.3 PO4.4 PO4.5 PO4.6 PO4.8 PO4.11 PO7.1 PO7.4 PO7.8 ME3.1	1. Is the IT department appropriately placed within the organisation, given the organisation's size and mission? 2. Is there an IT steering committee composed of executive, business and IT management and charged with ensuring business alignment (with supervision of IT plans and policies) and monitoring IT services and projects? 3. Are IT processes and IT-specific roles and responsibilities properly defined, exercised and monitored? 4. Have a local information security officer (LISO) and local security officer (LSO) been appointed in accordance with the Commission's regulatory framework? 5. Are there policies and procedures for managing staff recruitment and job termination? 6. Are the following roles segregated: a. Security: security officer (LSO and LISO) – system owner – security administrator (LSA-Local security administrator)? b. Changes: development – testing – quality assurance – production?		• IT process framework, documented roles and responsibilities • IT job descriptions • IT human resources policy and procedures • Decision or other document relating to the establishment of an IT steering committee • Sample minutes of IT steering committee meetings

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
5.	***Control objective:*** *Identify, prioritise, contain or accept relevant risks arising in the IT area and associated functions.* ***References to regulatory framework:*** *IR[5] Art. 48(e); ICS6 and ICS12* ***Related information criteria:*** *Confidentiality, integrity and availability*	PO9.1 PO9.2 PO9.3 PO9.4 PO9.5	1. Are IT risks managed in accordance with the organisation's risk management framework? 2. Is there an **IT-specific risk management framework**? 3. Are IT risks defined and monitored regularly in an **IT risk record** (separately or within the organisation's general risk record)?		• Risk management framework and/or policy • IT risk record/map
6.	***Control objective:*** *Identify, implement and monitor an internal control process for IT-related activities.* ***References to regulatory framework:*** *FR Art. 28a(2)(a,b,c); IR Arts 22a and 48(e); ICS9, ICS11, ICS 12 and ICS15* ***Related information criteria:*** *Effectiveness and efficiency*	ME2.1 ME2.2 ME2.7 ME3.1	1. Has a set of IT controls aligned with the organisation's internal control framework been established? 2. Has a set of IT controls designed to mitigate IT risks been identified? 3. Is there regular monitoring of and reporting on the effectiveness of IT controls? 4. Does the organisation of IT conform to the applicable rules and regulations in areas such as data protection and intellectual property rights? 5. Have any internal or external audit reports been produced on IT topics?		• Documentation of internal IT controls or the organisation's internal control standards (e.g. the ICS at the European Commission) • Audit reports in the field of IT (last 3 years)

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002R2342:20070501:EN:PDF

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
7.	***Control objective:*** *Define a programme and project management approach that is applicable to all IT projects, enables stakeholder participation and monitors project risks and progress.* ***References to regulatory framework:*** *ICS7* ***Related information criteria:*** *Effectiveness and efficiency*	PO10.2 PO10.3 AI2.2 AI4.3 AI4.4	1. Is there an IT project management methodology? 2. Are IT projects managed in line with the project management methodology? 3. Are new IT systems developed in line with a software development methodology (e.g. RUP@EC)?		• Project management guideline/ documentation • Software development methodology
8.	***Control objective:*** *Monitor and report process metrics and identify and implement performance improvement actions.* ***References to regulatory framework:*** *IR Art. 22a(1)(e); ICS9 and ICS15* ***Related information criteria:*** *Effectiveness and efficiency*	ME.1.1 ME.1.4 ME.1.5 ME.4.1 ME.4.2	1. Are senior management (or the steering committee) given regular **progress reports** on the overall contribution made by IT to the business so that they can monitor the extent to which the planned objectives have been achieved, budgeted resources have been used, performance targets have been met and identified risks have been mitigated?		• Regular progress reports

B. DATA MANAGEMENT CONTROLS

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
1.	***Control objective:*** *Ensure that data are properly stored, archived and disposed of.* ***References to regulatory framework:*** *FR Art. 28a(2)(b,c); IR Arts 22a(1)(d), 48(f,g), 107 and 108; ICS10, ICS11, ICS12 and ICS13* ***Related information criteria:*** *Integrity*	DS11.2 DS11.4 DS11.5 DS11.6	1. Are there policies established to store documents, data and source programmes in accordance with the organisation's activities, size and mission? 2. Do adequate policies and procedures exist for the backup of systems, applications, data and documentation: a. Do backup procedures provide guarantees of data recovery (with frequencies, copies, verifications, etc.) and correspond to the business continuity plan? b. Are all relevant data backed up (e.g. by means of audit logs, documents, spreadsheets)? c. Is there well-defined logical and physical security for data sources and backup copies? d. Has responsibility been assigned for the making and monitoring of backups? 3. Are systems, applications, data and documentation maintained or processed by third parties adequately backed up and/or secured? 4. Does the organisation have policies to ensure the protection of sensitive data and software when data and hardware are disposed of or transferred? 5. Are the retention periods for data in line with contractual, legal and regulatory requirements?		• Data management policy • Backup procedures • Procedures for disposal of media • Contracts with third parties or service-level agreements (data management clauses)

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
2.	***Control objective:*** *Establish an enterprise data model incorporating a data classification scheme to ensure the integrity and consistency of all data.* ***References to regulatory framework:*** *FR Art. 28a(2)(b,c); IR Arts 22a(1)(d), 48(c,f) and 107; ICS11, ICS12 and ICS13* ***Related information criteria:*** *Confidentiality and integrity*	PO2.3 PO2.4 DS5.11 DS11.1	1. Has a data dictionary been defined so that data redundancy/incompatibility can be identified and data elements can be shared among applications and systems? 2. Is the data dictionary applied to existing systems, application development projects and major changes to IT applications? 3. Are owners identified for each data element (files, folders, applications, etc.)? 4. Are data classified by information criterion: a. **confidentiality** (public, limited, etc.); b. **integrity** (moderate, sensitive, etc.); c. **availability** (moderate, critical, etc.)? 5. Is there a document showing the classification of each data element in accordance with the data classification scheme?		• Data management policy • Data classification scheme • Assigned data classifications • Data dictionary
3.	***Control objective (non-COBIT):*** *Ensure reliable production of financial and management information.* ***References to regulatory framework:*** *FR Arts 28a2(b) and 61(e);* ***IR Art. 48 (f);*** *ICS12 and ICS13* ***Related information criteria:*** *Confidentiality and integrity*	AC2 AC5	1. Have controls been designed to ensure the reliability of computerised data, including controls over **source documents**? 2. Have controls been designed to ensure the **integrity** and **security** of documents or files (such as spreadsheets) which are kept on personal computers or shared drives and are relied on by the organisation in its financial workflow where: a. those files are used to gather financial data or make calculations and serve as a basis for **manual entries in financial systems** (e.g. ABAC) **instead of source documents**? b. the files are used for **financial reporting**?		

C. BUSINESS CONTINUITY CONTROLS

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
1.	***Control objective:*** *Build the capabilities to carry out day-to-day automated business activities with minimal, acceptable interruption.* ***References to regulatory framework:*** *FR Art. 28a(2)(c);* *IR Art. 48(c); ICS10* ***Related information criteria:*** *Availability and effectiveness*	DS2.5 DS4.2 DS4.3 DS4.4 DS4.5	**1.** Are there a written and formally approved **business continuity plan (BCP)** and **disaster recovery plan (DRP)**? 2. Does the BCP cover: a. Business impact analysis (BIA)? b. All key business functions and processes? c. Roles, responsibilities and communication processes? 3. Are BCP tests scheduled and completed on a regular basis? 4. Is the BCP kept updated so that it continually reflects actual business requirements? 5. Are all critical backup media, documentation, data and other IT resources necessary for IT recovery stored offsite? 6. Do the BCP and DRP define recovery point objectives (**RPOs**) and recovery time objectives (**RTOs**)? 7. Are backup policies defined in accordance with RPOs and RTOs?		• BCP and DRP • Test reports

NB: in the absence of a suitable BCP the audited entity should be advised of the risk without delay.

D. INFORMATION SECURITY CONTROLS

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
1.	***Control objective:*** *Establish and maintain IT security roles, responsibilities, policies, standards and procedures.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Art. 48(c); ICS12* ***Related information criteria:*** *Confidentiality, integrity and effectiveness*	PO6.3 DS5.1 DS5.2	1. Has an IT security policy and/or plan been drawn up and approved at the appropriate level? 2. Does the **IT security plan** include/cover the following: a. A complete set of security policies and standards in line with the established IT security policy framework? b. Procedures for implementing and enforcing those policies and standards? c. Roles and responsibilities? d. Staffing requirements? e. Security awareness and training? f. Enforcement procedures? g. Investment in the necessary security resources?		• IT security policy and/or plan • Relevant security policies and procedures
2.	***Control objective:*** *Implement procedures for controlling access based on the individual's need to view, add, change or delete data.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Art. 48(c); ICS12* ***Related information criteria:*** *Confidentiality and integrity*	DS5.3 DS5.4	1. Are there procedures for defining access rights (view/add/change/delete) to financial systems (ABAC, etc.) and data/documents?		• User access rights policy/ user management policy • Access control lists (for financial systems and data)

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
3.	***Control objective:*** *Ensure that all users (internal, external and temporary) and their activity on IT systems are uniquely identifiable.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Art. 48(c); ICS12* ***Related information criteria:*** *Confidentiality and integrity*	DS5.3 AC6	1. Are there authentication and authorisation mechanisms, such as passwords, tokens or digital signatures, for enforcing access rights according to the sensitivity and criticality of information? 2. Are IDs unique and individual and passwords known only to the persons concerned?		
4.	***Control objective:*** *Controls on the appropriate segregation of duties for requesting and granting access to systems and data exist and are followed.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Art. 48(c); ICS8* ***Related information criteria:*** *Confidentiality and integrity*	DS5.3 DS5.4 PO4.11	1. Are user access rights requested by user management, approved by system/data owners and implemented by the *security administrator*? 2. Are the following roles segregated: a. ***Infrastructure***: security officer (LSO and LISO) – system owner – security administrator (implementing access by LSA etc.)? b. ***Applications***: system owner (authorisation and monitoring) – security administrator (e.g. profile administrator in ABAC)?		• Access control lists (for financial systems and data) • Job descriptions

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
5.	***Control objective:*** *Make sure one person (security administrator) is responsible for managing all user accounts and security tokens (passwords, cards, devices, etc.) and that appropriate emergency procedures are defined. Periodically review/confirm his/her actions and authority.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Art. 48(c); ICS8 and ICS12* ***Related information criteria:*** *Confidentiality and integrity*	DS5.4 DS13.4	1. Is there a *security officer* in charge of the organisation's IT security who obtains his/her authority from the senior management? 2. Is only the *security officer* able to manage user accounts and passwords? 3. Are the actions of the *security administrator* periodically reviewed (by the LISO), attention being given to the segregation of duties?		• Job descriptions of security officer and security administrator
6.	***Control objective:*** *Provide and maintain a suitable physical environment to protect IT assets from access, damage or theft.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Arts 48(c) and 108; ICS12* ***Related information criteria:*** *Confidentiality and integrity*	DS12.2 DS12.3 DS12.5	1. Has a policy been defined, and is it implemented, concerning the physical security and access control measures that are to be followed to prevent fire, water damage, power outages, theft, etc. at IT premises? 2. Is access to IT premises (IT rooms and facilities) granted, limited and revoked in accordance with physical security policies? 3. Is there a procedure for logging and monitoring all access to IT premises (including by contractors and vendors)?		• Policies relating to physical security

E. CHANGE MANAGEMENT CONTROLS

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
1.	***Control objective:*** *Control the impact assessment, authorisation and implementation of all changes to IT infrastructure, applications and technical solutions; minimise errors due to incomplete request specifications; and halt implementation of unauthorised changes.* ***References to regulatory framework:*** *IR Arts 22a(1)(d) and 107; ICS8* ***Related information criteria:*** *Integrity, availability, effectiveness and efficiency*	AI6.1 AI6.2 AI6.3 AI6.4 AI6.5 AI6.6	1. Is there a formally approved, implemented and monitored framework/procedures for managing changes to IT applications, programs and databases? 2. Does the change management framework include/cover: a. Roles and responsibilities? b. Change request procedures? c. The assessment of risks and the impacts of changes? d. Management authorisation for change requests? e. Approval by the key stakeholders, such as users and system owners, before changes move into production? f. Management review and approval of changes before they move into production? g. The classification of changes (major, minor, emergency changes, etc.)? h. The tracking of changes? i. Version control mechanisms? j. The definition of rollback procedures? k. The use of emergency change procedures? l. Audit trails?		• Change management framework/ procedures • All records of a sample of changes (from change request log to move into production)

			3. Are the following criteria for the segregation of duties respected in the context of program changes: a. Is the segregation of duties for development, testing, quality assurance and production tasks clearly established? b. Do program developers and testers conduct activities on "test" data only? 4. Do end users or system operators have direct access to program source codes?		
2	***Control objective:*** *Test that applications and infrastructure solutions are fit for the intended purpose and free from errors, and that adequate data conversion has occurred.* ***References to regulatory framework:*** *IR Arts 22a(1)(d) and 107; ICS8* ***Related information criteria:*** *Effectiveness*	AI7.2 AI7.6	1. Are all major changes tested against functional and operational requirements to ensure that original business goals are achieved? 2. Are all major changes executed in accordance with a test plan which covers: a. Organisational standards, roles and responsibilities? b. Test preparation, including site preparation? c. Training requirements, if needed? d. Installation or update of a defined test environment? e. Planning/performance/documentation/retention of test cases? f. Error and problem handling? g. Correction and escalation? h. Formal approval? 3. Are tests implemented on the live production system or in a test environment?		• Test plans and other documents relevant to the testing of a major change to an IT application/ program

F. CONTROLS ON OUTSOURCING IT INFRASTRUCTURE

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
1.	***Control objective:*** *Identify services delivered by IT. Define, agree upon and regularly review service-level agreements, which should cover service support requirements, related costs, roles and responsibilities, etc., and be expressed in business terms.* ***References to regulatory framework:*** *FR Art. 28a(2)(c); IR Arts 22a(1)(d), 48(c,f) and 108; ICS5, ICS8, ICS10, ICS11 and ICS12* ***Related information criteria:*** *Confidentiality, integrity, efficiency and effectiveness*	DS1.1	1. Are there clearly-defined benefits and business objectives in support of the decision to outsource? 2. Are management requirements and expectations clearly defined in the contract/SLA? 3. Were the risks assessed when deciding to outsource and taken into account when specifying the necessary controls? 4. Was the IT project carried out in accordance with existing project management standards?		• Contract(s) • SLA(s)
		AI 4.1 AI 5.2 DS1.3 DS1.6 DS2.4	5. Does the contract/SLA clearly define security requirements: a. Network security? b. Physical security? c. Anti-virus protection? d. Logical access controls?		
			6. Are the data backup requirements clearly defined? 7. Are provisions included for business continuity procedures? 8. Is there a clause on compliance with personal data protection regulations?		

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
			9. Does the contract/SLA give a detailed description of the service to be provided: a. Hardware and software requirements? b. Service support (help desk, incident management, problem management)? c. Maintenance and change management? d. IT staffing needs?		
			10. Does the contract/SLA include/cover the following: a. Formal management and legal approval? b. Costs, with specifications for payment (including frequency)? c. The principal roles and responsibilities? d. User/provider communications procedure and frequency? e. Contract duration? f. Problem resolution procedures? g. Non-performance penalties? h. The contract dissolution procedure? i. The contract modification procedure? j. Non-disclosure guarantees? k. Right to access and right to audit?		

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
2.	***Control objective:*** *Continuously monitor specified service-level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to stakeholders.* ***References to regulatory framework:*** *IR Art. 22a(1)(e); ICS9 and ICS15* ***Related information criteria:*** *Efficiency and effectiveness*	DS1.5 ME1.4 ME1.5 ME1.6	1. Does the contract/SLA define reporting procedures as regards the type, content, frequency and distribution of reports? 2. Is a procedure in place for continuous monitoring and regular reporting on the achievement of objectives? 3. Have formal performance criteria been established to facilitate and measure the achievement of the SLA objectives?		• Monitoring report(s)

5.2 *List of application controls*

Note: The following is a general outline of application controls (source: "IT Assurance Guide Using COBIT"[6] and "COBIT and Application Controls"[7]). In the case of robust IT applications, the auditor should identify other application controls in accordance with the financial regulatory framework after evaluating the complexity of the application and the related IT risks.

A. SOURCE DATA PREPARATION AND AUTHORISATION

Control Objectives	Application control requirements
Control Objective: *Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents.* *Errors and omissions can be minimised through good input form design.* *Detect errors and irregularities so they can be reported and corrected.* ***References to regulatory framework:*** *IR Art. 22a(1)(d), 48 (f) and 107; ICS7, ICS12 and ICS13.* ***Related information criteria:*** *Integrity and efficiency.*	**1.** Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents. **2.** Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction. **3.** Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures. **4.** Ensure that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management. **5.** Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction. **6.** Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

[6] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Assurance-Guide-Using-COBIT.aspx

[7] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-and-Application-Controls-A-Management-Guide.aspx

B. SOURCE DATA COLLECTION AND ENTRY

Control Objectives	Application control requirements
Control Objective: *Ensure that data input is performed in a timely manner by authorised and qualified staff.* *Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels.* *Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.* ***References to regulatory framework:*** *IR Art. 22a(1)(d), 48 (f,g), and 107; ICS7 and ICS13.* ***Related information criteria:*** *Integrity*	**1.** Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria. **2.** Use only pre-numbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents. **3.** Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions. **4.** Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in a timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels. **5.** Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time. **6.** Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and, where necessary, incidents are raised for more senior-level attention. Automated monitoring tools should be used to identify, monitor and manage errors. **7.** Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.

C. ACCURACY, COMPLETENESS AND AUTHENTICITY CHECKS

Control Objectives	Application control requirements
Control Objective: *Ensure that transactions are accurate, complete and valid.* *Validate data that were input, and edit or send back for correction as close to the point of origination as possible.* ***References to regulatory framework:*** *FR Art. 28a (2)(b,c) and 61(e); IR Art. 22a(1)(a,d), 48 (c,f),and 107; ICS7, ICS12 and ICS13.* ***Related information criteria:*** *Integrity and efficiency.*	**1.** Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately to enable efficient remediation. **2.** Implement controls to ensure accuracy, completeness, validity and compliance to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation. **3.** Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data. **4.** Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements. **5.** Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion and do not delay processing of valid transactions. **6.** Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

D. PROCESSING INTEGRITY AND VALIDITY

Control Objectives	Application control requirements
Control Objective: *Maintain the integrity and validity of data throughout the processing cycle.* *Detection of erroneous transactions does not disrupt the processing of valid transactions.* ***References to regulatory framework:*** *FR Art. 28a (2) (b,c) and 61(e); IR Art. 22a(1) (a,d), 48 (c,f),and 107; ICS7, ICS12 and ICS13.* ***Related information criteria:*** *Integrity, confidentiality, and availability.*	**1.** Establish and implement mechanisms to authorise the initiation of transaction processing and to ensure that only appropriate and authorised applications and tools are used. **2.** Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow. **3.** Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or prevent errors. **4.** Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled. **5.** Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing. **6.** Verify the unique and sequential identifier to every transaction (e.g., index, date and time). **7.** Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made. **8.** Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed. **9.** Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry. **10.** Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify,, report and act upon out-of-balance conditions.

E. OUTPUT REVIEW, RECONCILIATION AND ERROR HANDLING

Control Objectives	Application control requirements
Control Objective: *Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; verification, detection and correction of the accuracy of output occur; and information provided in the output is used.* ***References to regulatory framework:*** *FR Art. 28a 2(b,c), Art. 61(e); IR Art. 48 (f) and 108; ICS7, ICS12 and ICS13.* ***Related information criteria:*** *Integrity, confidentiality, availability and effectiveness.*	**1.** When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output. **2.** At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents. **3.** Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management. **4.** Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses. **5.** Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and output is handled in line with the applicable confidentiality classification. Report potential errors; log them in an automated, centralised logging facility; and address errors in a timely manner. **6.** If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

F. TRANSACTION AUTHENTICATION AND INTEGRITY

Control Objectives	Application control requirements
Control Objective: *Before passing transaction data between internal applications and business/ operational functions (within or outside the enterprise), check the data for proper addressing, authenticity of origin and integrity of content.* *Maintain authenticity and integrity during transmission or transport.* ***References to regulatory framework:*** *FR Art. 28a 2(c) and 48 (f); ICS7, ICS12 and ICS13.* ***Related information criteria:*** *Integrity and confidentiality.*	**1.** Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled. **2.** Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation and allow for content integrity verification upon receipt by the downstream application. **3.** Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.

5.3 *IT Audit Glossary*

Access control list (ACL). An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals.

Access rights. The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy.

Application. A set of programs, data and clerical procedures which together form an information system designed to handle a specific administrative or business function (e.g. accounting, payment of grants, recording of inventory). Most applications can usefully be viewed as processes with input, processing, stored data, and output.

Audit trail. A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source.

Availability. The accessibility of a system, resource or file, where and when required. The time that a system is not available is called downtime. Availability is determined by reliability, maintainability, serviceability, performance, and security.

Backup. A duplicate copy (e.g. of a document or of an entire disc) made either for archiving purposes or for safeguarding valuable files from loss should the active copy be damaged or destroyed. A backup is an "insurance" copy.

Batch. A set of computer data or jobs to be processed in a single program run.

Buffer overflow. It occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Business continuity plan (BCP). A logistical plan to recover and restore the critical business operations within a predetermined time after a disaster or extended disruption. Some of the critical business operations need IT services to continue: these are the critical IT services. A part of the BCP is the Disaster Recovery Plan that addresses the restoration of the critical IT services.

Change management. The process responsible for controlling the lifecycle of all changes. The primary objective of change management is to enable beneficial changes to be made, with minimum disruption to IT Services.

Check digit. A numeric value, which has been calculated mathematically, is added to data to ensure that original data have not been altered or that an incorrect, but valid match has occurred.

Control objective. A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.

Data dictionary. A database that contains the name, type, source and authorization for access for each data element in the organisation's files and databases. It also indicates which application programmes use that data so that when a data structure is contemplated, a list of the affected programmes can be generated.

Disaster recovery plan (DRP). A plan used to restore the critical IT services in case of a disaster affecting IT infrastructure. A DRP is not valid unless tested at least once a year. The DRP is a part of the BCP.

Hash total. A figure obtained by some operations upon all the items in a collection of data and used for control purposes. A recalculation of the hash total, and comparison with a previously computed value, provides a check on the loss or corruption of the data.

Input. Information/data received by the computer system either from an external source or from another area within the computer environment.

Integrity. One of the information criteria that information is valid, complete and accurate.

IT governance. The responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.

IT risk. The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise

IT risk map. A tool for ranking and displaying IT risks by defined ranges for frequency and magnitude.

IT Steering Committee. Comprising of user representatives from all areas of the business, and IT. The steering committee would be responsible for the overall direction of IT. Involvement of the management in this committee is indispensable to assure business alignment in IT governance. The IT steering committee assists the executive in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects and focuses on implementation.

IT strategic plan. A long term plan, i.e., three to five year horizon, in which business and IT management cooperatively describe how IT resources will contribute to the enterprise's strategic objectives (goals).

Job description. A document which defines the roles, responsibilities, skills and knowledge required by a particular person.

Log. A log is to record details of information or events in an organized record-keeping system, usually sequenced in the order they occurred.

Logical access controls. The use of software to prevent unauthorized access to IT resources (including files, data, and programs) and the associated administrative procedures.

Output. Information/data produced by computer processing, such as graphic display on a terminal and hard copy.

Outsourcing. A formal agreement with a third party to perform a function for an organization.

Owner. The individual (or unit) responsible for particular (IS or IT) assets.

Recovery point objective (RPO). The RPO is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data.

Recovery time objective (RTO). The amount of time allowed for the recovery of a business function or resource after a disaster occurs.

Production environment. A controlled environment containing live configuration items used to deliver it services to customers.

Segregation of duties. is a control which aims to ensure that transactions are properly authorised, recorded, and that assets are safeguarded. It has two dimensions: separation of the responsibility for the controls of assets from the responsibility for maintaining the related accounting records; and separation of functions within the IT environment.

Sequence check. A verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research.

Service level agreement (SLA). A written agreement between the provider of a service and the users. A SLA contains "service level objectives" such as uptime (when an application must be available), and the acceptable response time. SLAs should exist between IT and the users for each service and application. SLAs must also be a part of the contract with external providers.

Source code. The text written in a computer programming language. The source code consists of the programming statements that are created by a programmer with a text editor or a visual programming tool and then saved in a file.

Source documents. The forms used to record data that have been captured. A source document may be a piece of paper, a turnaround document or an image displayed for online data input.

Token. A device that is used to authenticate a user, typically in addition to a username and password.

User. Individual or unit that makes use of information systems. Specifically, in business and administration, a managed organisational unit which uses information systems to carry out the functions for which it is responsible in the organization, and is thus the customer for a service provided by the IT department.

Validity check. Software control over input of data to a computer system. Data is compared with the type of data properly included in each input field, e.g., only letters in a name field.