# Checklist for IT 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.

This checklist for general controls 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](http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx) in reference to the EU's regulatory framework and information criteria in the areas of IT governance and management, data management, business continuity planning, information security, change management and outsourcing of IT infrastructure.

You can jump directly to the following sections of the checklist for general controls:

1. [IT governance and management](#_IT_GOVERNANCE_AND)
2. [Data management](#_DATA_MANAGEMENT_CONTROLS)
3. [Business continuity planning](#_BUSINESS_CONTINUITY_CONTROLS)
4. [Information security](#_INFORMATION_SECURITY_CONTROLS)
5. [Change management](#_CHANGE_MANAGEMENT_CONTROLS)
6. [Outsourcing of IT infrastructure](#_CONTROLS_ON_OUTSOURCING)

# 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: 2. Data management and classification? 3. Business continuity? 4. Information security? 5. Risks and controls? 6. Change management? |  | * Policies, procedures, guidelines and manuals |
| *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: 7. Security: security officer (LSO and LISO) – system owner – security administrator (LSA-Local security administrator)? 8. 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 |
| *5.* | ***Control objective:*** *Identify, prioritise, contain or accept relevant risks arising in the IT area and associated functions.*  ***References to regulatory framework:*** *IR 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) |
| *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 |

# 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: 3. Do backup procedures provide guarantees of data recovery (with frequencies, copies, verifications, etc.) and correspond to the business continuity plan? 4. Are all relevant data backed up (e.g. by means of audit logs, documents, spreadsheets)? 5. Is there well-defined logical and physical security for data sources and backup copies? 6. Has responsibility been assigned for the making and monitoring of backups? 7. Are systems, applications, data and documentation maintained or processed by third parties adequately backed up and/or secured? 8. Does the organisation have policies to ensure the protection of sensitive data and software when data and hardware are disposed of or transferred? 9. 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) |
| *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: 5. **confidentiality** (public, limited, etc.); 6. **integrity** (moderate, sensitive, etc.); 7. **availability** (moderate, critical, etc.)? 8. 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, with **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: 3. 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**? 4. the files are used for **financial reporting**? |  |  |

# 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: 3. Business impact analysis (BIA)? 4. All key business functions and processes? 5. Roles, responsibilities and communication processes? 6. Are BCP tests scheduled and completed on a regular basis? 7. Is the BCP kept updated so that it continually reflects actual business requirements? 8. Are all critical backup media, documentation, data and other IT resources necessary for IT recovery stored offsite? 9. Do the BCP and DRP define recovery point objectives(**RPOs**) and recovery time objectives(**RTOs**)? 10. 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.**

# 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: 3. A complete set of security policies and standards in line with the established IT security policy framework? 4. Procedures for implementing and enforcing those policies and standards? 5. Roles and responsibilities? 6. Staffing requirements? 7. Security awareness and training? 8. Enforcement procedures? 9. 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) |
| *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: 3. ***Infrastructure***: security officer (LSO and LISO) – system owner – security administrator (implementing access by LSA etc.)? 4. ***Applications***: system owner (authorisation and monitoring) – security administrator (e.g. profile administrator in ABAC)? |  | * Access control lists (for financial systems and data) * Job descriptions |
| *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* | DS12.2DS12.3 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 |

# 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: 3. Roles and responsibilities? 4. Change request procedures? 5. The assessment of risks and the impacts of changes? 6. Management authorisation for change requests? 7. Approval by the key stakeholders, such as users and system owners, before changes move into production? 8. Management review and approval of changes before they move into production? 9. The classification of changes (major, minor, emergency changes, etc.)? 10. The tracking of changes? 11. Version control mechanisms? 12. The definition of rollback procedures? 13. The use of emergency change procedures? 14. Audit trails? |  | * Change management framework/ procedures * All records of a sample of changes (from change request log to move into production) |
|  |  |  | 1. Are the following criteria for the segregation of duties respected in the context of program changes: 2. Is the segregation of duties for development, testing, quality assurance and production tasks clearly established? 3. 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: 3. Organisational standards, roles and responsibilities? 4. Test preparation, including site preparation? 5. Training requirements, if needed? 6. Installation or update of a defined test environment? 7. Planning/performance/documentation/retention of test cases? 8. Error and problem handling? 9. Correction and escalation? 10. Formal approval? 11. 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 |

# 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 | 1. Does the contract/SLA clearly define security requirements: 2. Network security? 3. Physical security? 4. Anti-virus protection? 5. Logical access controls? |  |
| 1. Are the data backup requirements clearly defined? 2. Are provisions included for business continuity procedures? 3. Is there a clause on compliance with personal data protection regulations? |  |
| 1. Does the contract/SLA give a detailed description of the service to be provided: 2. Hardware and software requirements? 3. Service support (help desk, incident management, problem management)? 4. Maintenance and change management? 5. IT staffing needs? |  |
| 1. Does the contract/SLA include/cover the following: 2. Formal management and legal approval? 3. Costs, with specifications for payment (including frequency)? 4. The principals' roles and responsibilities? 5. User/provider communications procedure and frequency? 6. Contract duration? 7. Problem resolution procedures? 8. Non-performance penalties? 9. The dissolution procedure? 10. The contract modification procedure? 11. Non-disclosure guarantees? 12. Right to access and right to audit? |  |
| *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) |