COBIT 2019 Framework – ITGC Checklist

TechEd Academy
Learn | Certify | Succeed

We are pleased to share Part 1 of the COBIT Checklist, carefully prepared to support your learning and understanding of the COBIT framework.

Whether you're a student, professional, or enthusiast in the field of IT governance, this checklist is designed to assist you in grasping the key components of COBIT in a clear and structured manner.

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

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
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

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
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

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		• 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

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
			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?		• 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 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)

	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

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
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

Thank You

Part 2 Coming Soon....

TechEd Academy
Learn | Certify | Succeed