COBIT 2019 Framework – ITGC Checklist

We are pleased to share Part 4 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.

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 regulatry 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?		• Change management framework/ procedures • All records of a sample of changes (from change request log to move into production)

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

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
			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? Do end users or system operators have direct access to program source codes?		

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
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?		Test plans and other documents relevant to the testing of a major change to an IT application/ program

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

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

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
			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 principals' roles and responsibilities? d. User/provider communications procedure and frequency? e. Contract duration? f. Problem resolution procedures? g. Non-performance penalties? h. The 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)

Thank You

TechEd Academy
Learn | Certify | Succeed