COBIT 2019 Framework – ITGC Checklist

We are pleased to share Part 3 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.

C. BUSINESS CONTINUITY CONTROLS

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

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

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?		• IT security policy and/or plan • Relevant security policies and procedures

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
			e. Security awareness and training? f. Enforcement procedures? g. Investment in the necessary security resources?		
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? Are IDs unique and individual and passwords known only to the persons concerned?		

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
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?		1. Job descriptions of security officer and security administrator

	Control objectives and reference to the regulatory framework	COBIT ref.	Tests of controls	Evaluation	Documents required
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? a. Is there a procedure for logging and monitoring all access to IT premises (including by contractors and vendors)?		2. Policies relating to physical security

Thank You

Part 4 (Final) Coming Soon....

TechEd Academy
Learn | Certify | Succeed