# Alles in één pagina

## [YouTube Video: COBIT Framework explained by Dr Phil](https://www.youtube.com/watch?v=Ei3-1KgjARA)

[](https://www.youtube.com/watch?v=Ei3-1KgjARA)

[(bron)](https://memegenerator.net/img/images/300x300/1139490.jpg)

## COBIT Framework introductie

COBIT is een door ISACA ontwikkeld IT-beheer framework dat bedrijven kan helpen bij het formuleren, organiseren en implementeren van informatiebeheer- en governance-strategieën. COBIT (Control Objectives for Information and Related Technologies) werd voor het eerst uitgebracht in 1996 en was oorspronkelijk ontworpen als een reeks IT-controledoelstellingen om de financiële auditgemeenschap te helpen beter te reageren op de groei van de IT-omgeving. In 1998 bracht ISACA versie 2 uit, waarmee het raamwerk werd uitgebreid tot buiten de auditgemeenschap. In de jaren 2000 ontwikkelde ISACA versie 3, waarin de technologieën voor IT-beheer en informatiebeheer die in het huidige framework worden gebruikt, worden gecombineerd. COBIT 4 werd uitgebracht in 2005, gevolgd door COBIT 4.1 in 2007. Deze updates bevatten meer informatie over het beheer van informatie- en communicatietechnologie ie. In 2012 werd COBIT 5 uitgebracht. In 2013 bracht ISACA COBIT 5-add-ons uit, die meer informatie bevatten over risico- en informatiebeheer voor ondernemingen. ISACA heeft in 2018 een bijgewerkte versie van COBIT uitgebracht, het versienummer verlaten en het COBIT2019 genoemd. Volgens ISACA streeft deze bijgewerkte versie van COBIT ernaar om zich voortdurend te ontwikkelen door middel van frequentere en soepelere updates. De introductie van COBIT2019 is om een governance-strategieën vast te stellen die flexibeler is, meer samenwerkt en reageert op nieuwe en veranderende technologieën.

![COBIT Logo](data:text/html; charset=iso-8859-1;base64,PCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9JRVRGLy9EVEQgSFRNTCAyLjAvL0VOIj4KPGh0bWw+PGhlYWQ+Cjx0aXRsZT40MDMgRm9yYmlkZGVuPC90aXRsZT4KPC9oZWFkPjxib2R5Pgo8aDE+Rm9yYmlkZGVuPC9oMT4KPHA+WW91IGRvbid0IGhhdmUgcGVybWlzc2lvbiB0byBhY2Nlc3MgdGhpcyByZXNvdXJjZS48L3A+CjwvYm9keT48L2h0bWw+Cg==)[(bron)](https://ab-audit.com/wp-content/uploads/2020/07/COBIT-2019-Design-and-Implementtion.png)

## Domeinen en aandachtsgebeiden

### Cloud domeinen

COBIT heeft raakvlak met alle cloud domeinen, dat zijn:

* Strategische besluitvorming
* Milieu
* Marktpositionering
* Financiën
* Operationele processen
* Veiligheid en naleving (compliance)

[(bron)](http://arno.uvt.nl/show.cgi?fid=144876)

### COBIT Domeinen

De IT-resources worden binnen COBIT beheerst door middel van 34 IT-processen die verdeeld zijn over vier domeinen;

* Planning en Organisatie (PO)
* Acquisitie en Implementatie (AI)
* Delivery en Support (DS)
* Monitoring

[(bron)](http://www.raamstijn.nl/eenblogjeom/index.php/informatiemanagement/363-cobit)

### Kwaliteitscriteria

Om organisatiedoelstellingen te realiseren dient informatie voor het aansturen van de organisatie en haar bedrijfsprocessen te voldoen aan zeven kwaliteitscriteria;

* Doeltreffendheid
* Efficiëntie
* Vertrouwelijkheid
* Integriteit
* Beschikbaarheid
* Naleving (compliance)
* Betrouwbaarheid.

[(bron)](http://www.raamstijn.nl/eenblogjeom/index.php/informatiemanagement/363-cobit)

## Uitgangspunten en resultaten

Door de vijf uitgangspunten van COBIT (uit de onderstaande afbeelding) kunnen de volgende resulaten een gevolg zijn van de implementatie; een goed rendement op investeringen in IT-gerelateerde bedrijfsinvesteringen. Bevorderd beheer van IT-gerelateerde bedrijfsrisico’s, bedrijfsveranderingen, product- en bedrijfsinnovatie. Ook zorgt het voor continuïteit van de dienstverlening en beschikbaarheid. Het creëert flexibiliteit om te reageren op veranderende bedrijfsbehoeften, het bereikt kostenoptimalisatie van de dienstverlening en resulteert in lagere proceskosten. [(bron)](http://arno.uvt.nl/show.cgi?fid=144876) [(bron)](https://i.pinimg.com/originals/53/a2/13/53a213645436189d1df328bfe7a88960.jpg)

### 1. Voldoen aan behoeften van stakeholders

Het eerste principe van de COBIT-formule is om tegemoet te komen aan de belangen en behoeften van stakeholders. Het is gebaseerd op het idee dat het bestaan van een bedrijf is om waarde te creëren voor belanghebbenden. Stakeholders hebben bepaalde eisen, die vertaald moeten worden naar organisatiedoelstellingen. Bij het nemen van beslissingen met betrekking tot het IT-beheer van de organisatie, moeten belanghebbenden zich bewust zijn van en deelnemen aan dit proces.

### 2. Organisatie afdekken end-to-end

Het tweede principe benadrukt dat controle en risicomanagement voor de hele organisatie gelden, inclusief alle. Alle functies en processen met betrekking tot de informatie moeten worden opgenomen.

### 3. Een enkel geïntegreerd raamwerk toepassen

Het derde principe is om één integratiekader in te zetten. Dit kan organisaties helpen om de meeste waarde uit IT-oplossingen te halen. Daarnaast kan COBIT worden gebruikt als totaalsysteem voor frameworks als BiSL en COSO.

### 4. Holistische benadering mogelijk maken

Het vierde principe gaat over het mogelijk maken van een holistische benadering. Dit betekent het gebruik van een launcher. Deze bijdragende factoren bepalen of bepaalde dingen werken. COBIT 5 heeft zeven factoren die de governance van enterprise IT-governance (GEIT) bevorderen:

* Principes
* Beleid
* Kaders
* Processen
* Cultuur
* Informatie
* Mensen

### 5. Bestuur scheiden van management

Het vijfde en laatste principe van COBIT 5 is om de raad van bestuur te scheiden van het management. COBIT benadrukt de noodzaak om onderscheid te maken tussen governance en management, omdat ISACA gelooft dat deze twee componenten aparte structuren en processen vereisen.

## Positie van het Framework

COBIT heeft een hoge positie in business frameworks en is erkend onder verschillende internationale standaarden waaronder ITIL, CMMI, COSO, PRINCE2, TOGAF, PMBOK, TOGAF en ISO 27000. Het fungeert als een richtlijnintegrator die alle oplossingen samenvoegt onder één paraplu. [(bron)](https://itmunch.com/cobit-framework-alignment-governance/)

[(bron)](https://3.bp.blogspot.com/-TDaYRn2YJQE/Vq0R2nAB7JI/AAAAAAAATho/CNxtJuOkpdg/s1600/AAEAAQAAAAAAAAJ6AAAAJGM5OWU3M2VmLWM3ZDYtNGQ5MS05MTliLWE3NWJmNGU5M2JkYg.jpg)

## Voor- en nadelen

Hoewel COBIT 5 wordt geprezen voor de integratie van andere ISACA-best practices, wordt het ook bekritiseerd vanwege een aantal tekortkomingen. Hoewel COBIT 5 veel verbetering vertoont ten opzichte van de vorige versie COBIT 4.1, zou de complexiteit ervan nieuwe gebruikers kunnen afschrikken. Dit kan de invoering ervan belemmeren, aangezien nieuwe gebruikers op hun hoede kunnen zijn en bedenkingen hebben. Het onderzoeksbureau Gartner Inc. legt uit dat het COBIT framework “de vervagende grens tussen operationele technologie en informatietechnologie negeert, wat een toenemende invloed zal hebben op het beheer van risico’s en het leveren van waarde, en extra controles zal vereisen”. Zij stellen ook dat de verdedigers van COBIT 5 hun kritiek weerleggen met het argument dat Gartner & Co het framework niet begrijpt en er niet in slaagt de richtlijnen voor het beheer van informatie en technologie te herkennen. [(bron)](https://www.henryharvin.com/blog/faqs-about-cobit-5/)

## COBIT bij publieke cloud aanbieders

Alle publieke cloud aanbieders doen wat risk management. AWS heeft een strategisch bedrijfsplan ontwikkeld dat onder meer voorziet in het identificeren van risico’s en het implementeren van controles om risico’s te beperken of te beheren. De controleomgeving van AWS is onderworpen aan verschillende interne en externe risicoanalyses. AWS Compliance en Security teams hebben een informatiebeveiligingsraamwerk en -beleid opgesteld dat gebaseerd is op de Control Objectives for Information and Related Technology (COBIT).

Microsoft Azure daarentegen gebruikt als beveiligingsstrategie dat er altijd sprake is van een inbreuk op de systemen en services. Microsoft Azure heeft veel methoden om de gegevens van klanten te beveiligen: Auditing en logging, cybercriminaliteit, ontwerp- en operationele beveiliging, encryptie, identiteits- en toegangsbeheer, netwerkbeveiliging en bedreigingsbeheer.

GCP biedt ook een set van modellen, zoals informatiebeveiligingsteam, fysieke beveiliging in datacenters, server- en softwarestapelbeveiliging, gegevensbeveiliging en vele platformbeveiligingsfuncties. Met de focus op de compliance die Microsoft Azure en GCP bieden voor hun diensten, voldoen zij aan de volgende kaders en certificeringen die hierin worden genoemd papier: ISO 9000/27000-serie, ISAE 3402 SOC 1/2/3 en zij voltooiden de Cloud Security Alliance STAR Self-Assessment.