

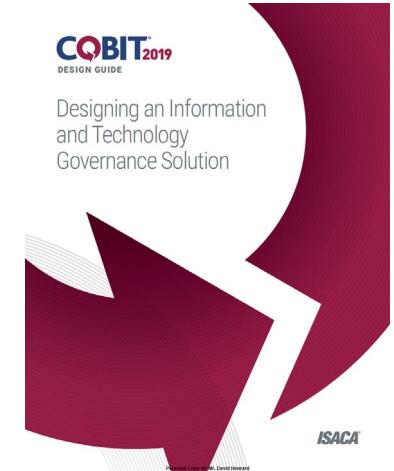
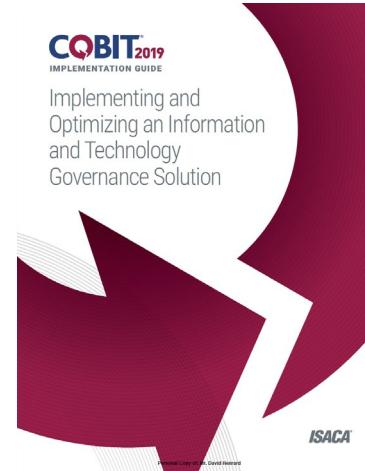
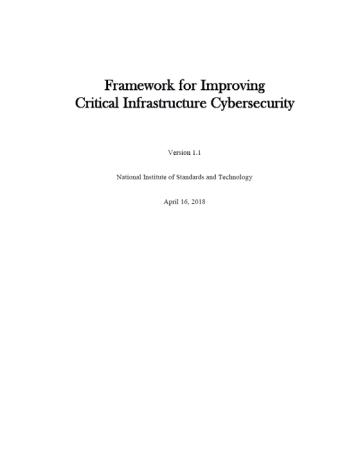
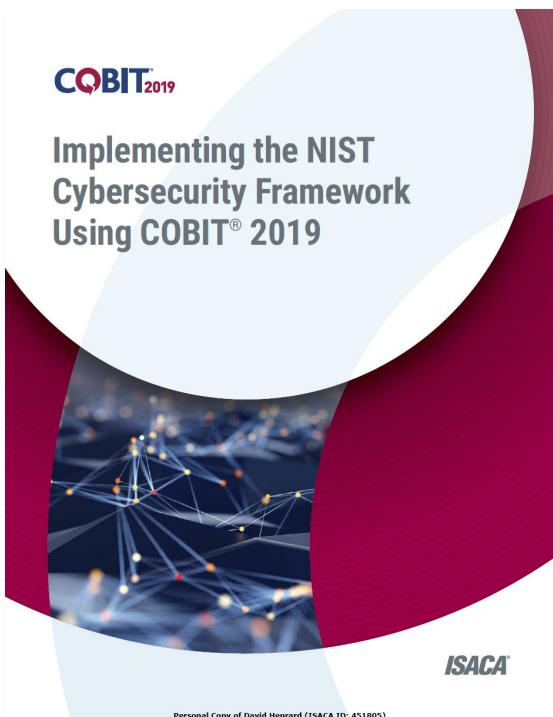


IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK 1.1 USING COBIT 2019

PRÉSENTATION DU GUIDE

David Henard, CISA, CISM, CRISC, CGEIT

PORTÉE DU GUIDE



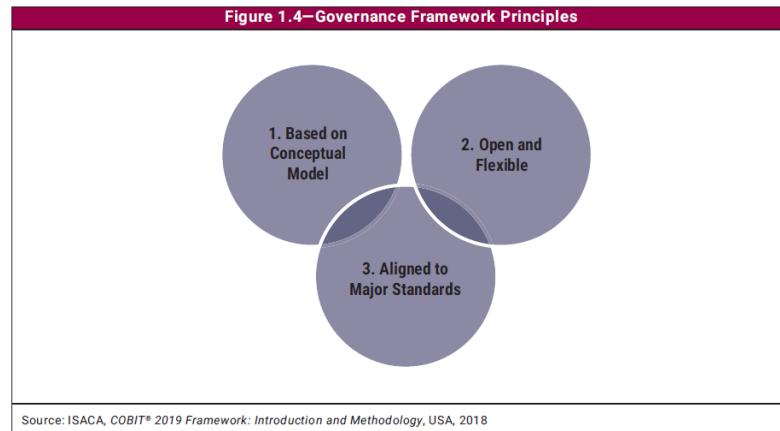
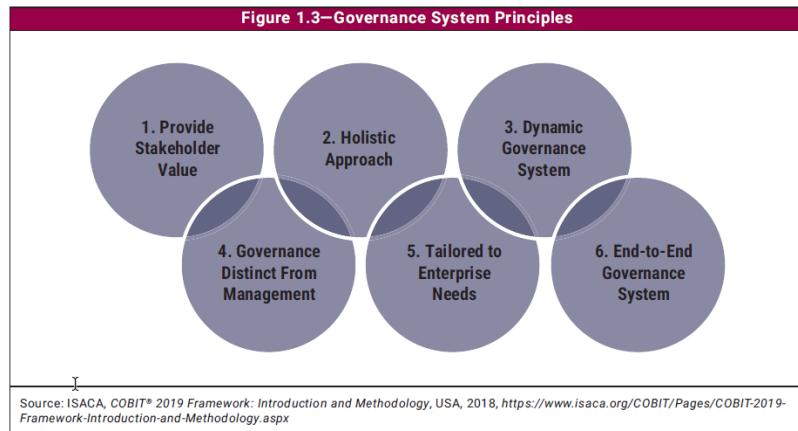
QU'EST-CE QUE LE CSF DU **NIST** ?

- Ensemble de lignes directrices destiné à permettre aux organisations de faire face aux risques de cybersécurité



QU'EST-CE QUE COBIT[®]₂₀₁₉ ?

- COBIT est un référentiel pour la gouvernance et la gestion de l'information et des technologies de l'entreprise.



LES 3 COMPOSANTES DU CSF

- **Cœur du référentiel**

Les résultats souhaités en matière de cybersécurité sont organisés de manière hiérarchique et alignés sur des orientations et des contrôles plus détaillés

- **Profils**

Alignement des exigences et des objectifs d'une organisation, de son appétit pour le risque et de ses ressources en utilisant les résultats souhaités du cadre de base

- **Niveaux de mise en œuvre**

Une mesure qualitative des pratiques organisationnelles de gestion des risques de cybersécurité

(Partiel, informé des risques, répétable, adaptatif)



LE CŒUR – FONCTIONS ET CATÉGORIES

IDENTIFY						PROTECT			DETECT			RESPOND				RECOVER						
Asset Management	Business Environment	Governance	Risk Assessment	Risk Management	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements	Recovery Planning	Improvements	Communications

EDM01—Ensured Governance Framework Setting and Maintenance

EDM02—Ensured Benefits Delivery

EDM03—Ensured Risk Optimization

EDM04—Ensured Resource Optimization

EDM05—Ensured Stakeholder Engagement

COBIT[®] 2019

AP001—Managed I&T Management Framework

AP002—Managed Strategy

AP003—Managed Enterprise Architecture

AP004—Managed Innovation

AP005—Managed Portfolio

AP006—Managed Budget and Costs

AP007—Managed Human Resources

AP008—Managed Relationships

AP009—Managed Service Agreements

AP010—Managed Vendors

AP011—Managed Quality

AP012—Managed Risk

AP013—Managed Security

AP014—Managed Data

BAI01—Managed Programs

BAI02—Managed Requirements Definition

BAI03—Managed Solutions Identification and Build

BAI04—Managed Availability and Capacity

BAI05—Managed Organizational Change

BAI06—Managed IT Changes

BAI07—Managed IT Change Acceptance and Transitioning

BAI08—Managed Knowledge

BAI09—Managed Assets

BAI10—Managed Configuration

BAI11—Managed Projects

DSS01—Managed Operations

DSS02—Managed Service Requests and Incidents

DSS03—Managed Problems

DSS04—Managed Continuity

DSS05—Managed Security Services

DSS06—Managed Business Process Controls

MEA01—Managed Performance and Conformance Monitoring

MEA02—Managed System of Internal Control

MEA03—Managed Compliance With External Requirements

MEA04—Managed Assurance

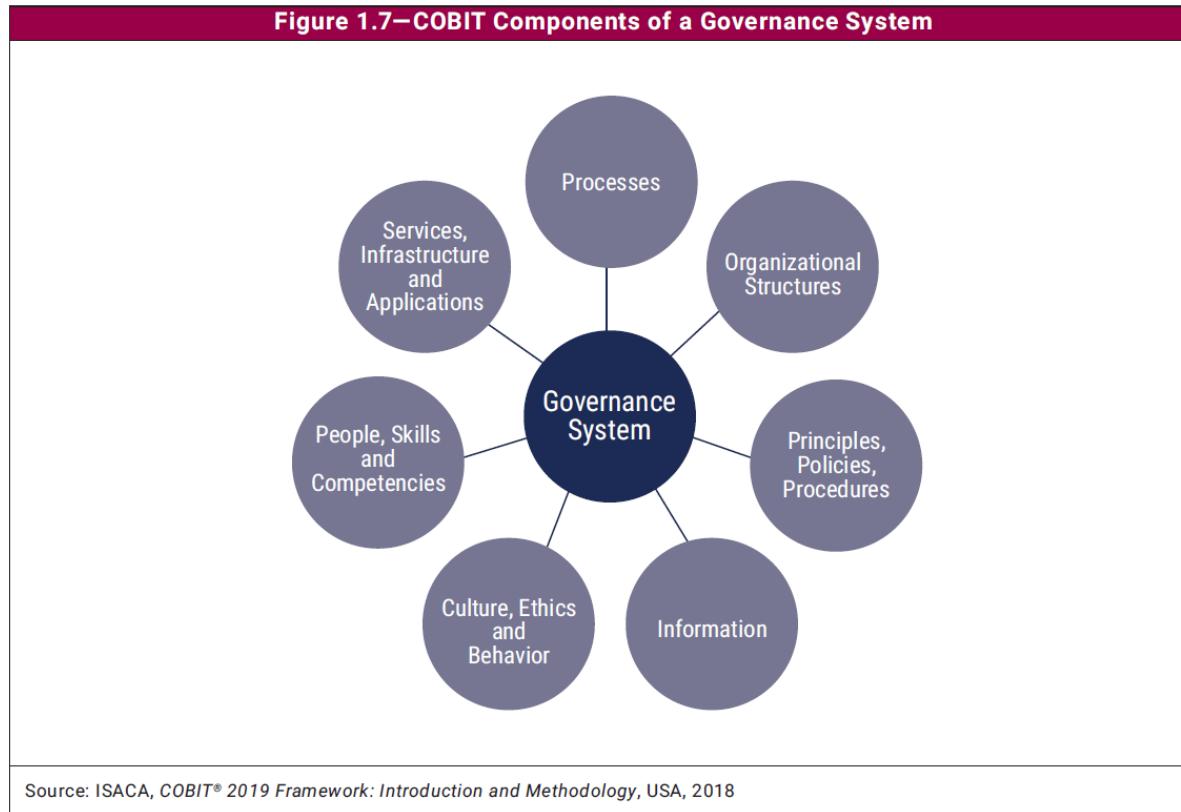
Governance objectives

NIST CYBER

Management objectives

IF

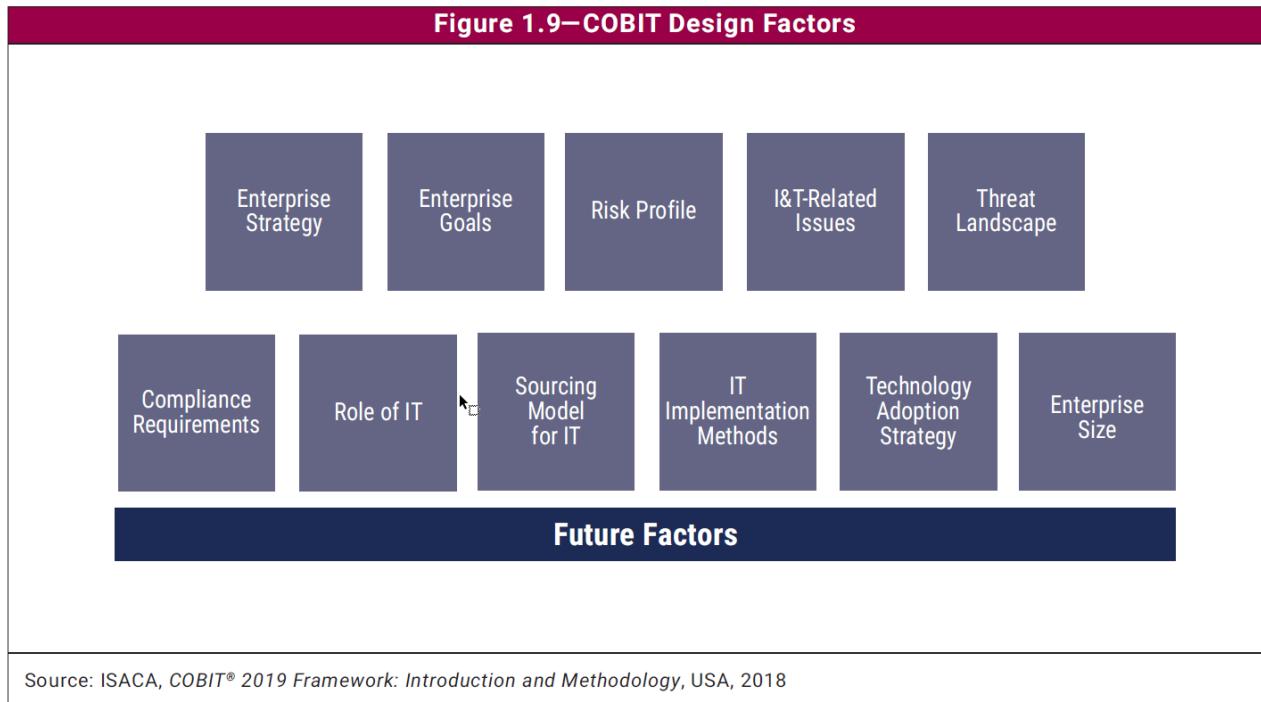
LES COMPOSANTS D'UN SYSTÈME DE GOUVERNANCE



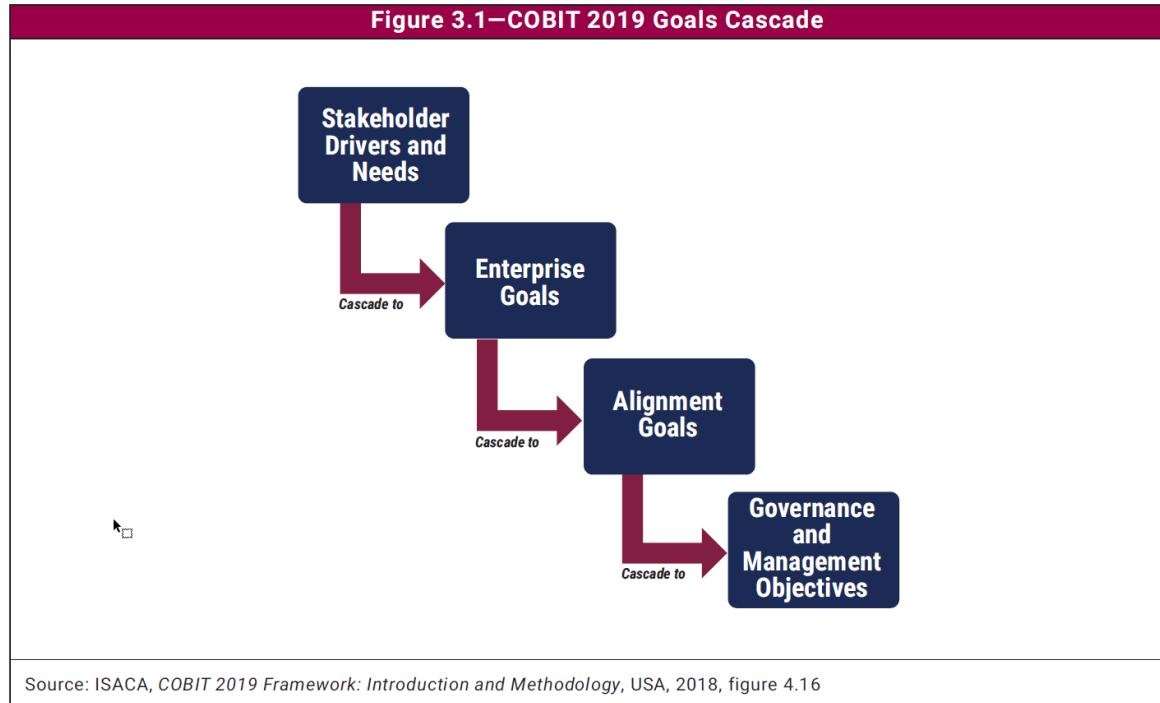
IMPLEMENTING THE NIST CSF TOOLKIT

CSF Framework				Current Profile	
A	B	C	D	E	F
1	Function	Category	Subcategory	Implementation Status	Org Practices
2	IDENTIFY (ID) Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. +	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. +	ID.AM-1: Physical devices and systems within the organization are inventoried	COBIT 2019 BAI09.01, BAI09.02	
3			ID.AM-2: Software platforms and applications within the organization are inventoried	COBIT 2019 BAI09.01, BAI09.02, BAI09.05	
4			ID.AM-3: Organizational communication and data flows are mapped	COBIT 2019 APO14.08, DSS05.02	
5			ID.AM-4: External information systems are catalogued	COBIT 2019 APO02.02, APO10.01, APO10.04, DSS01.02	
6					
7					

LES FACTEURS DE CONCEPTION DE COBIT



RELATIONS ENTRE LA CASCADE D'OBJECTIFS DE COBIT ET LE CSF



COBIT 2019 IMPLEMENTATION PHASES / CSF 1.1 IMPLEMENTATION STEPS

NIST CSF 1.1 Implementation Steps	COBIT 2019 Implementation Phases	COBIT 2019 Design Guide Steps		
1. Prioritize and Scope	1. What Are the Drivers?	Understand the Enterprise Context and Strategy		
2. Orient	2. Where Are We Now?	Determine the Initial Scope of the Governance System	Determine the Initial Scope of the Governance System	Resolve Conflicts and Conclude the Governance System Design
3. Create a Current Profile				
4. Conduct a Risk Assessment	3. Where Do We Want to Be?			
5. Create a Target Profile				
6. Determine, Analyze, and Prioritize Gaps	4. What Needs to Be Done?			
7. Implement Action Plan	5. How Do We Get There?			
NIST CSF Lifecycle Action Plan Review	6. Did We Get There?			
NIST CSF Lifecycle Management	7. How Do We Keep the Momentum Going?			

POUR ALLER PLUS LOIN

The screenshot shows the COBIT 2019 website. At the top, there's a large maroon banner with the COBIT 2019 logo. To its right, the text "Governance at Your Fingertips" and a subtext "Build your expertise in the globally accepted framework for optimizing enterprise IT governance." Below this is a green navigation bar with three tabs: "Why COBIT", "Publications", and "Certification and Training". On the left, there's a sidebar with social sharing icons (Facebook, Twitter, LinkedIn, etc.) and a "1.3k Shares" counter. The main content area features a section titled "A right-sized governance solution...tailor-fit for your enterprise." followed by a paragraph about COBIT 2019 being the most recent evolution of ISACA's framework. Below this is a section titled "EFFECTIVE GOVERNANCE" with a target icon and a paragraph about effective governance over information and technology. At the bottom, there's a section titled "MORE IMPLEMENTATION RESOURCES" with a gear icon and a paragraph about updated implementation resources, practical guidance, and training opportunities. A red button labeled "ACCESS THE COBIT TOOLKIT" is also present.

<https://www.isaca.org/resources/cobit>



<https://engage.isaca.org/>

+



David Henrard, CISA, CISM, CRISC, CGEIT

david.henrard@infidem.biz

<https://www.linkedin.com/in/davidhenrard/>

<https://infidem.biz/>

+

+

+