IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK 1.1 USING COBIT 2019

PRÉSENTATION DU GUIDE

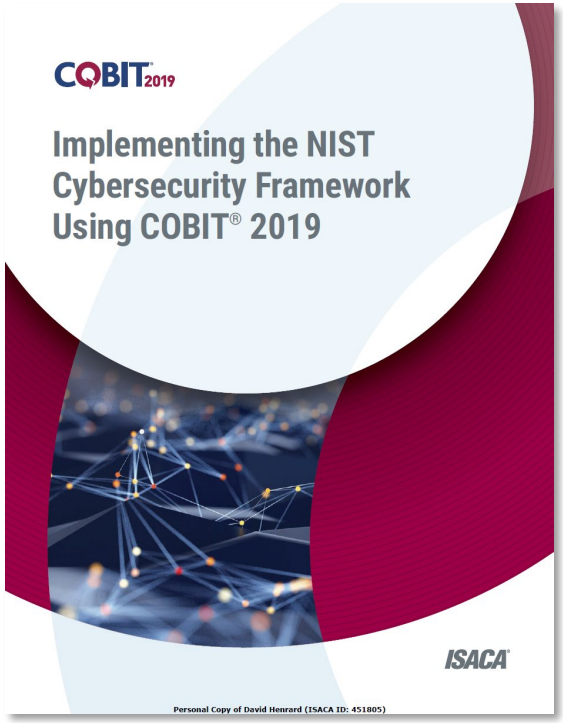
David Henrard, CISA, CISM, CRISC, CGEIT

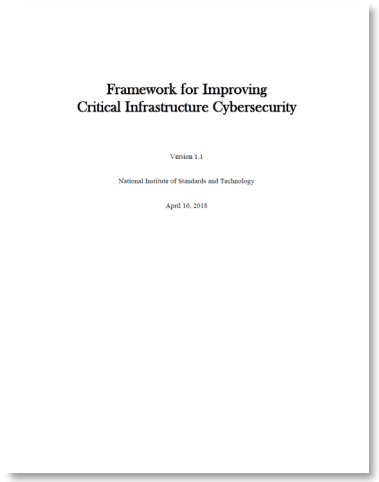
ISACA Section de Québec

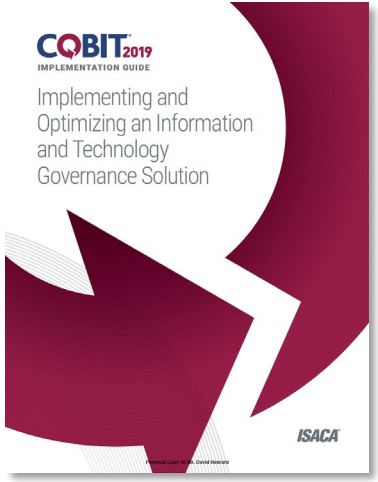
27 octobre 2020 – ISACA Québec – In Fidem

IF

PORTÉE DU GUIDE







ISACA Section de Québec

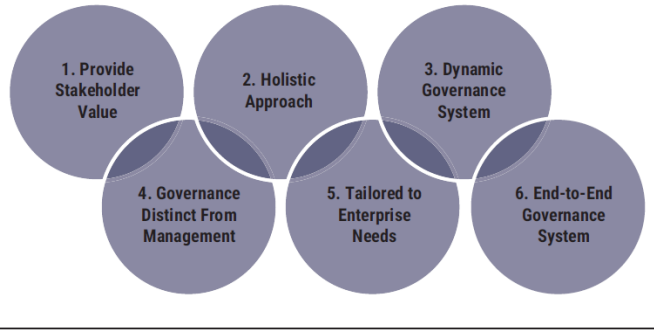
QU'EST-CE QUE LE CSF DU NIST ?

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

QU'EST-CE QUE COBIT 2019 ?

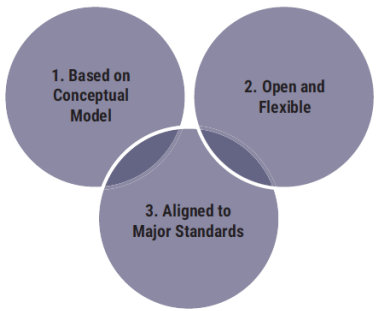
- COBIT est un référentiel pour la gouvernance et la gestion de l'information et des technologies de l'entreprise.

Figure 1.3—Governance System Principles



Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Introduction-and-Methodology.aspx*

Figure 1.4—Governance Framework Principles



Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018

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**

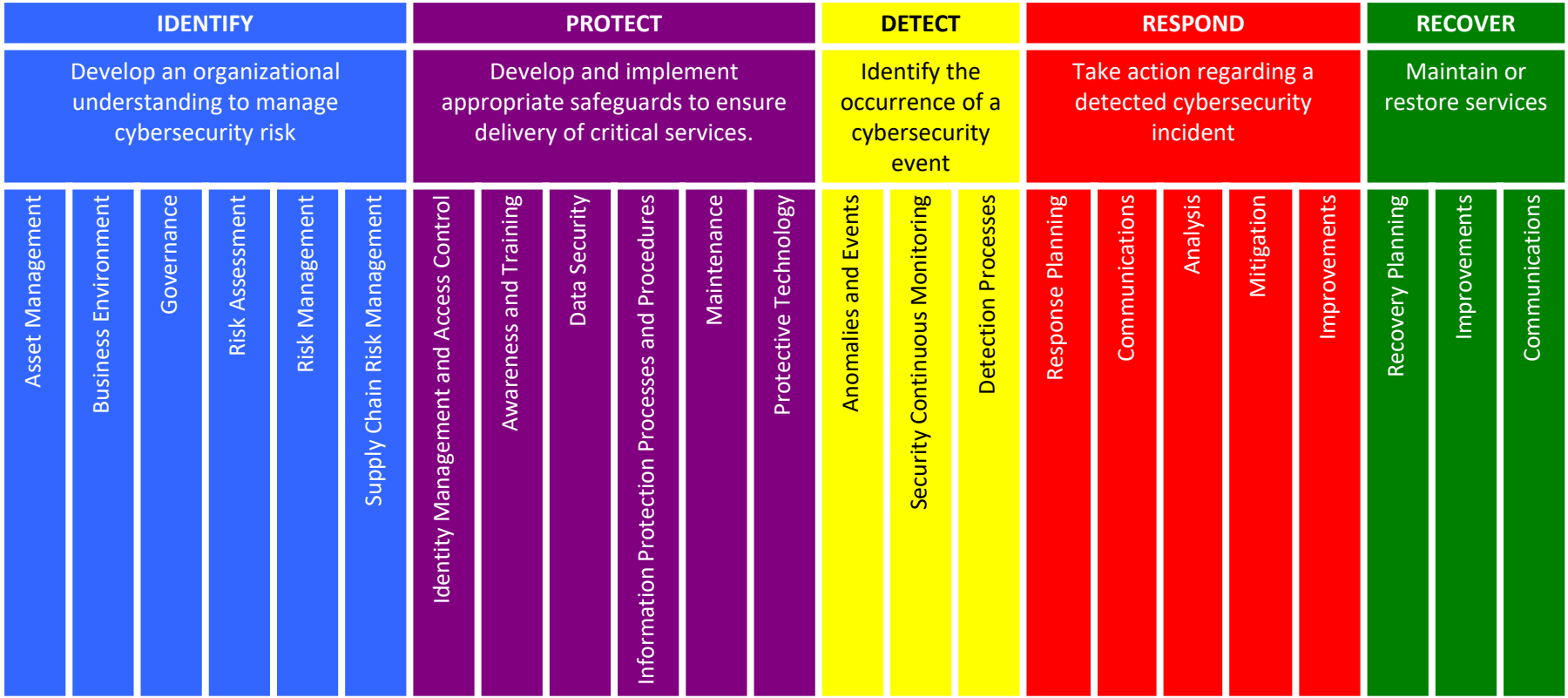
  Alignement des exigences et des objectifs d'une organisation, de son appétit pour le risque et de ses ressources en utilisant les résultats souhaités du cadre de base

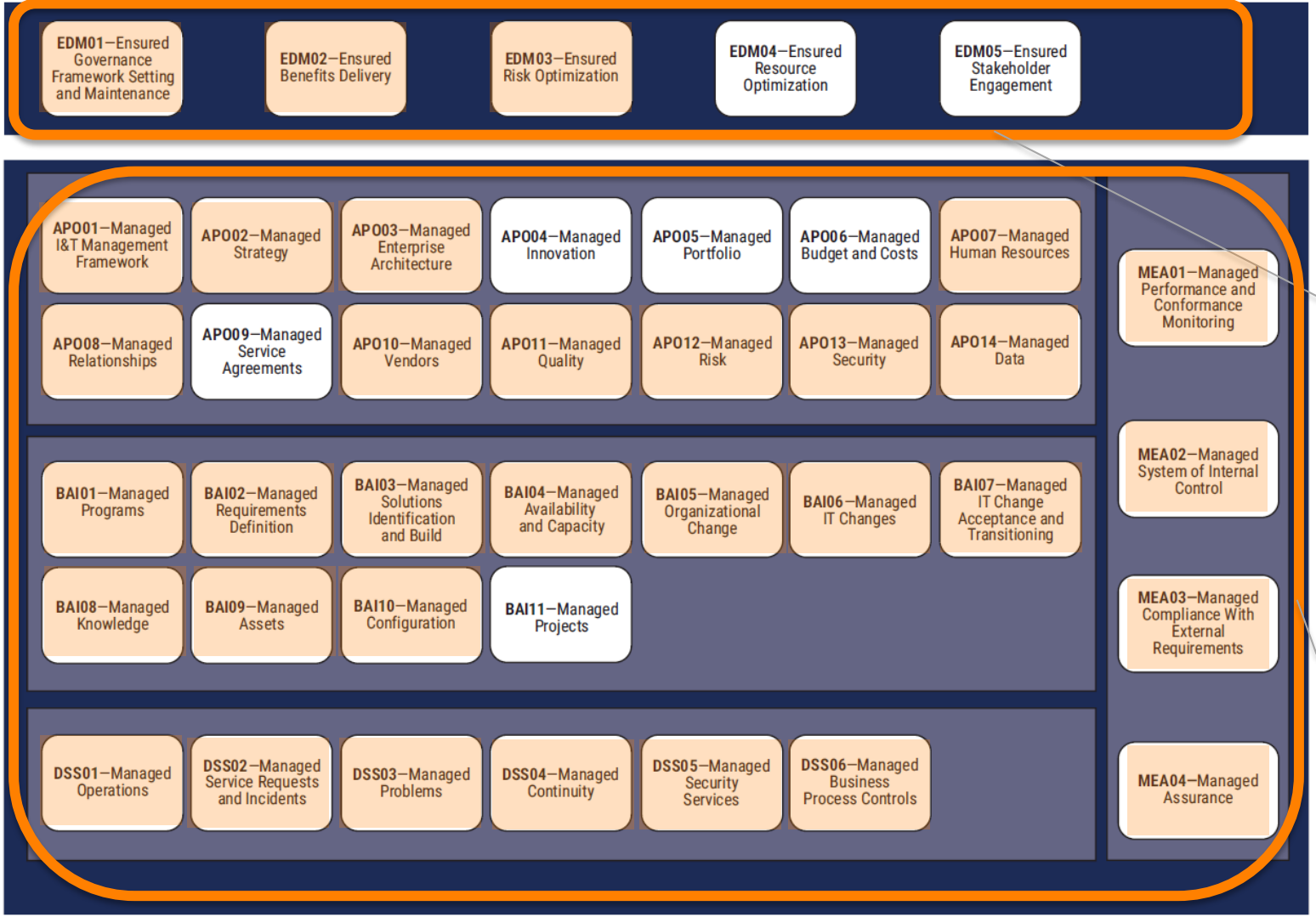
- **Niveaux de mise en œuvre**

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

  (Partiel, informé des risques, répétable, adaptatif)

LE CŒUR – FONCTIONS ET CATÉGORIES





COBIT 2019

Governance objectives

Management objectives

NIST CYBER

IF

LES COMPOSANTS D'UN SYSTÈME DE GOUVERNANCE

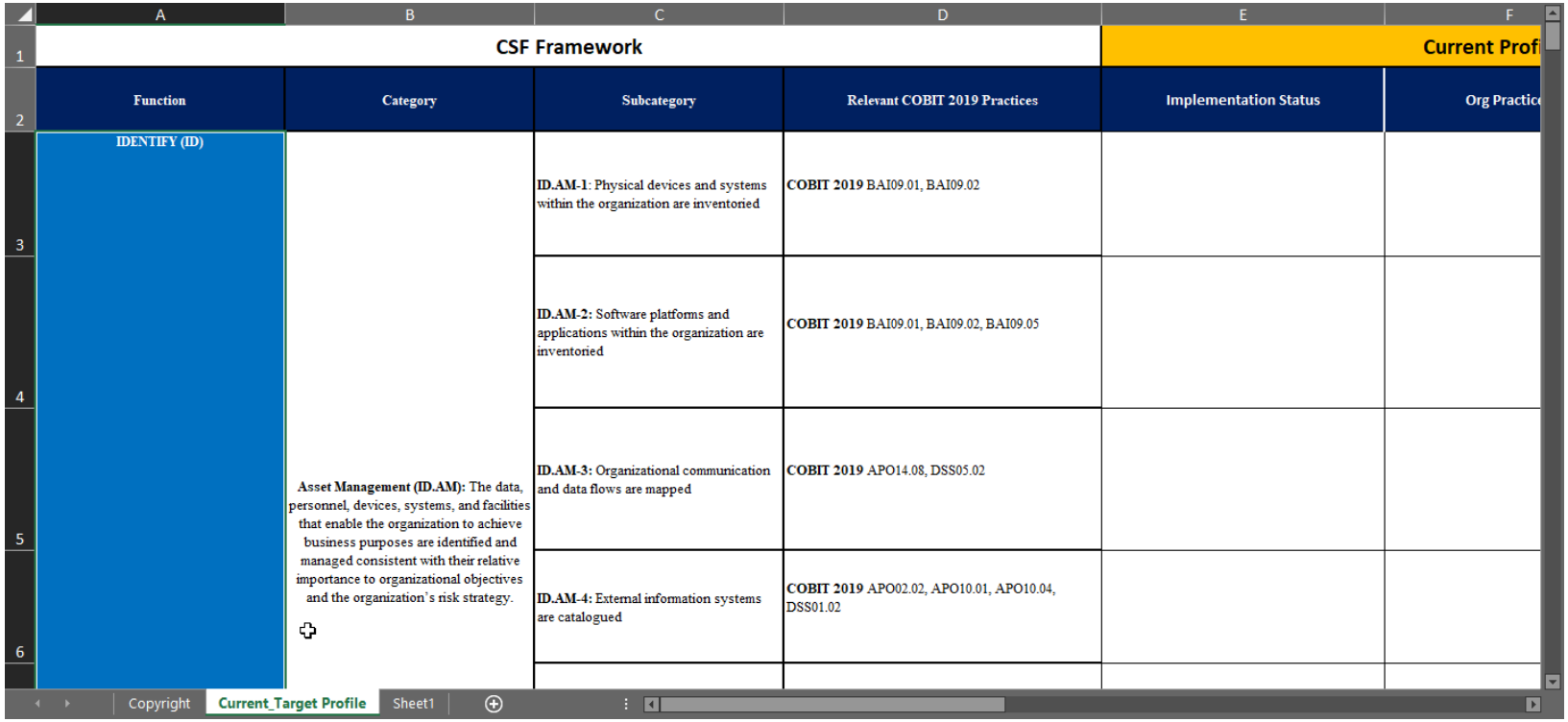
Figure 1.7—COBIT Components of a Governance System

Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018

ISACA Section de Québec

IF

IMPLEMENTING THE NIST CSF TOOLKIT



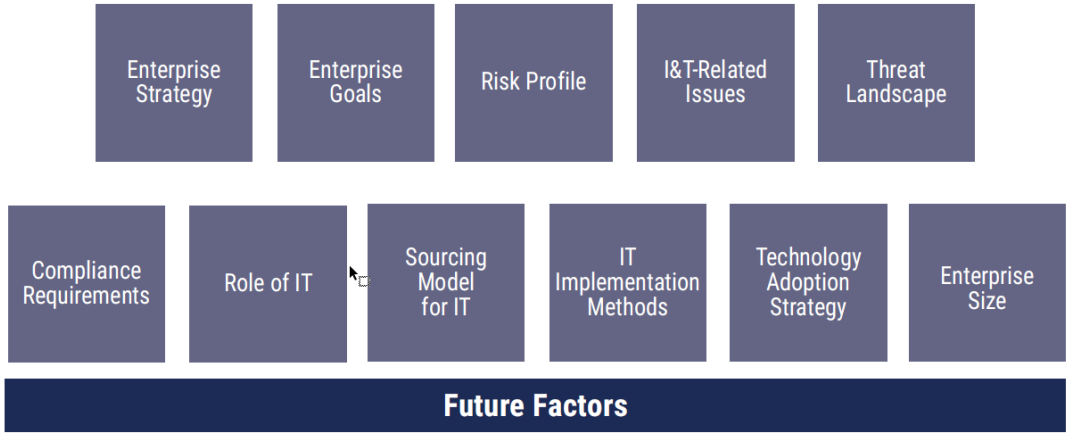
	A	B	C	D	E	F
1	CSF Framework				Current Profi	
2	Function	Category	Subcategory	Relevant COBIT 2019 Practices	Implementation Status	Org Practic
3	IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified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

Copyright | Current_Target Profile | Sheet1

ISACA Section de Québec

LES FACTEURS DE CONCEPTION DE COBIT

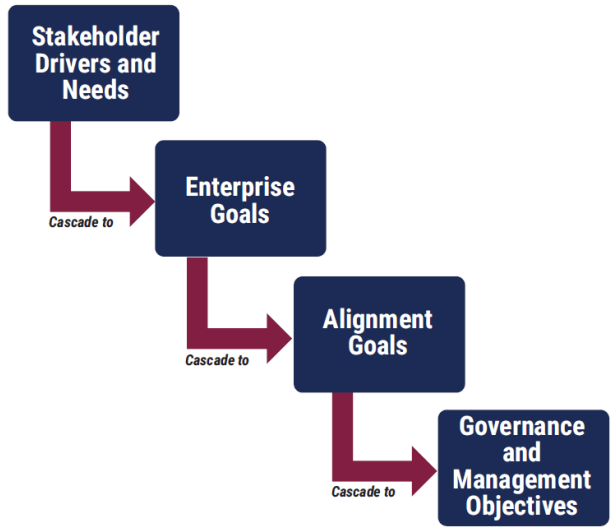
Figure 1.9—COBIT Design Factors



Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018

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

Figure 3.1—COBIT 2019 Goals Cascade



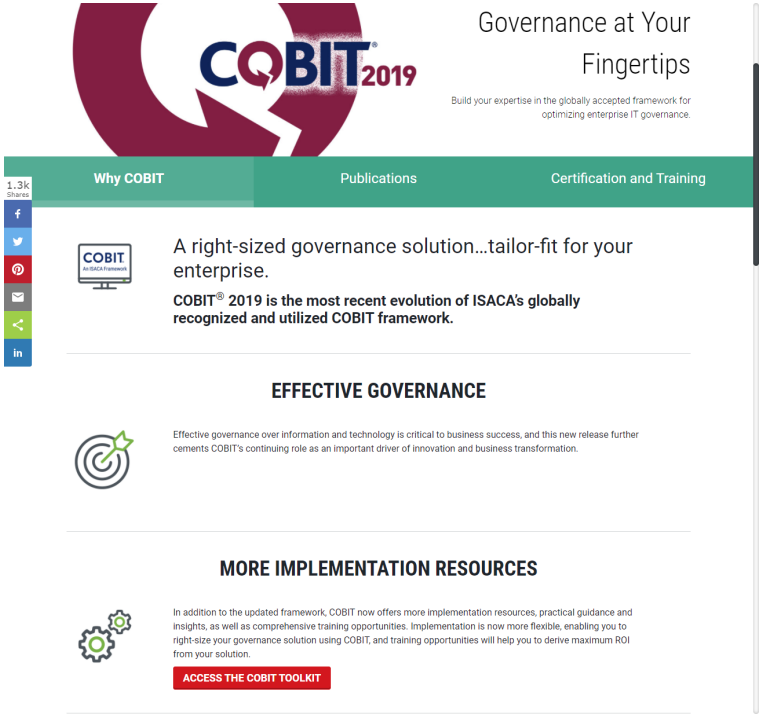
Source: ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, figure 4.16

ISACA Section de Québec

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



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

COBIT®
An ISACA® Framework
ISACA | ENGAGE

https://engage.isaca.org/

David Henrard, CISA, CISM, CRISC, CGEIT

david.henrard@infidem.biz

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

https://infidem.biz/