Comité de la Comunidad Valenciana

itSMF ESPAÑA

ISACA Sistemas de información fiables y valiosos

Valencia Chapter

Cloud vs. ISO20K & 27K "sin llegar a las manos"

21 de Junio de 2012

Cómo hacer nudos de corbata … o ¿Qué me pongo hoy?

Jaume Siscar Bondia

CISA, CISM, CGEIT, CRISC, LA ISO 27000

Director de Certificaciones ISACA Valencia

itSMF

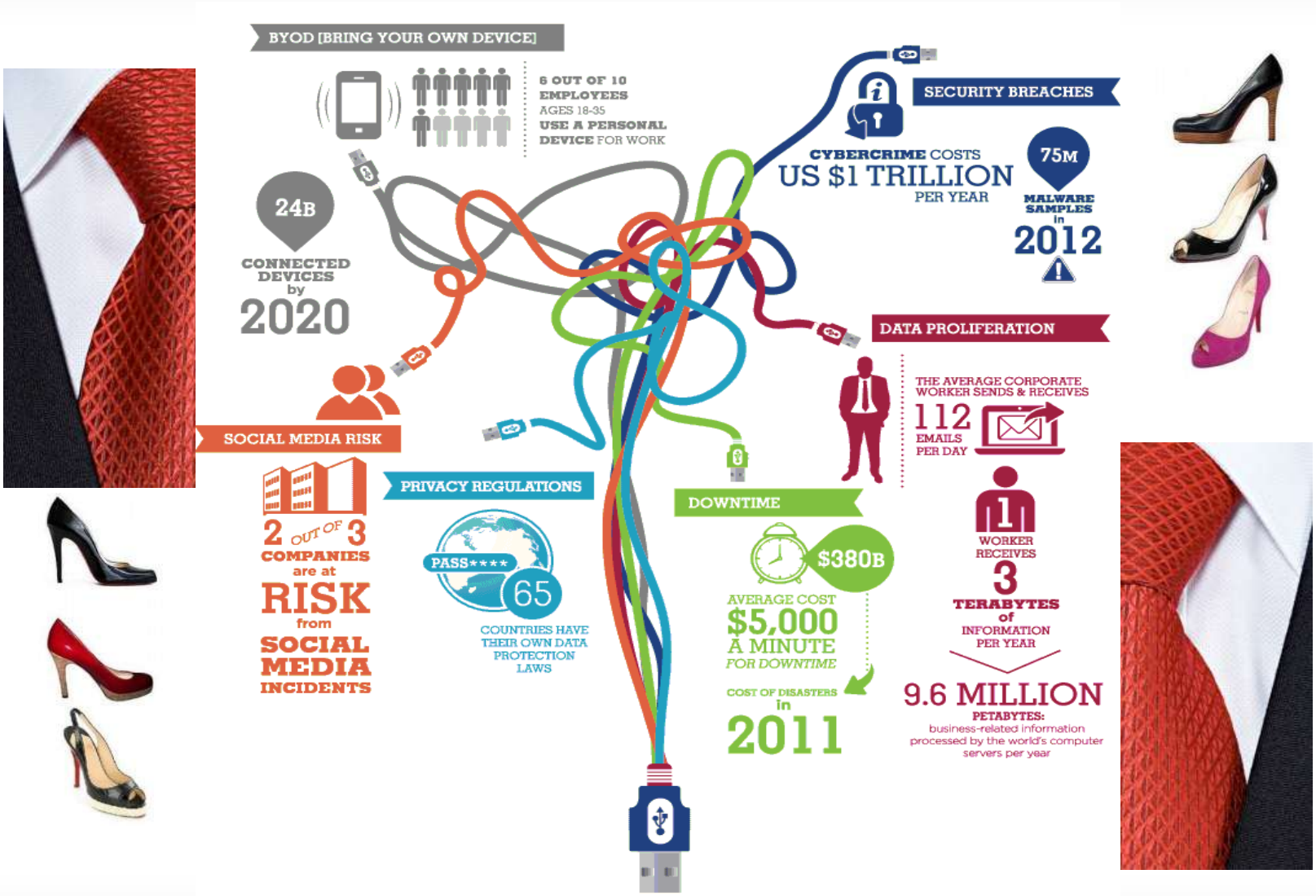
Introducción

Cloud vs. ISO20K & 27K
“sin llegar a las manos”

¿Dónde?

Cloud vs. ISO20K & 27K
“sin llegar a las manos”

¿Dónde?



Cloud vs. ISO20K & 27K
"sin llegar a las manos"

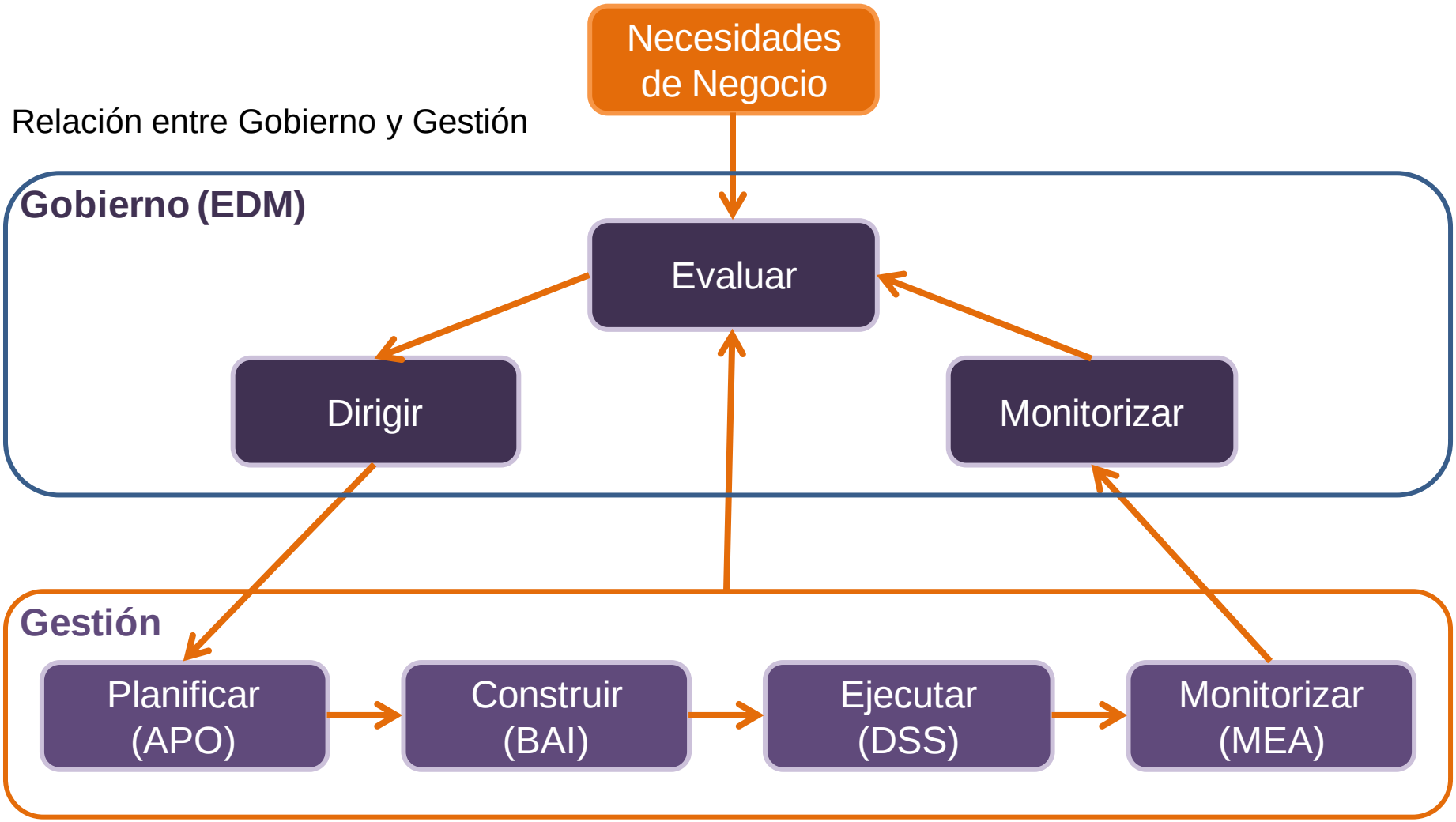
¿Dónde?

El **Gobierno** asegura que se logran los objetivos de la empresa mediante la evaluación de las necesidades, condiciones y opciones de los interesados, realiza el ajuste de dirección a través de la priorización, la toma de decisiones y el seguimiento del desempeño de los objetivos (EDM).

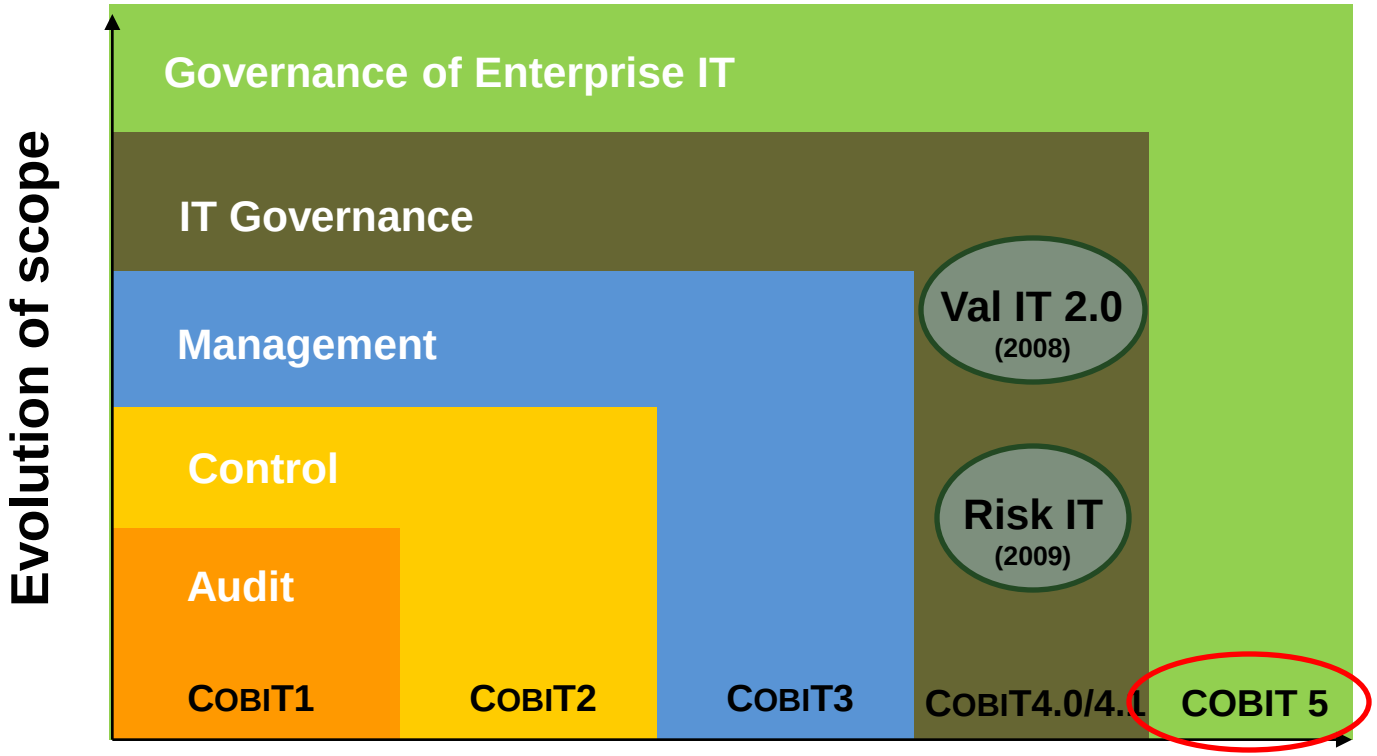
La **Gestión** planifica, construye, ejecuta y monitoriza las actividades en alineación con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa (PBRM).

¿Dónde?

Relación entre Gobierno y Gestión

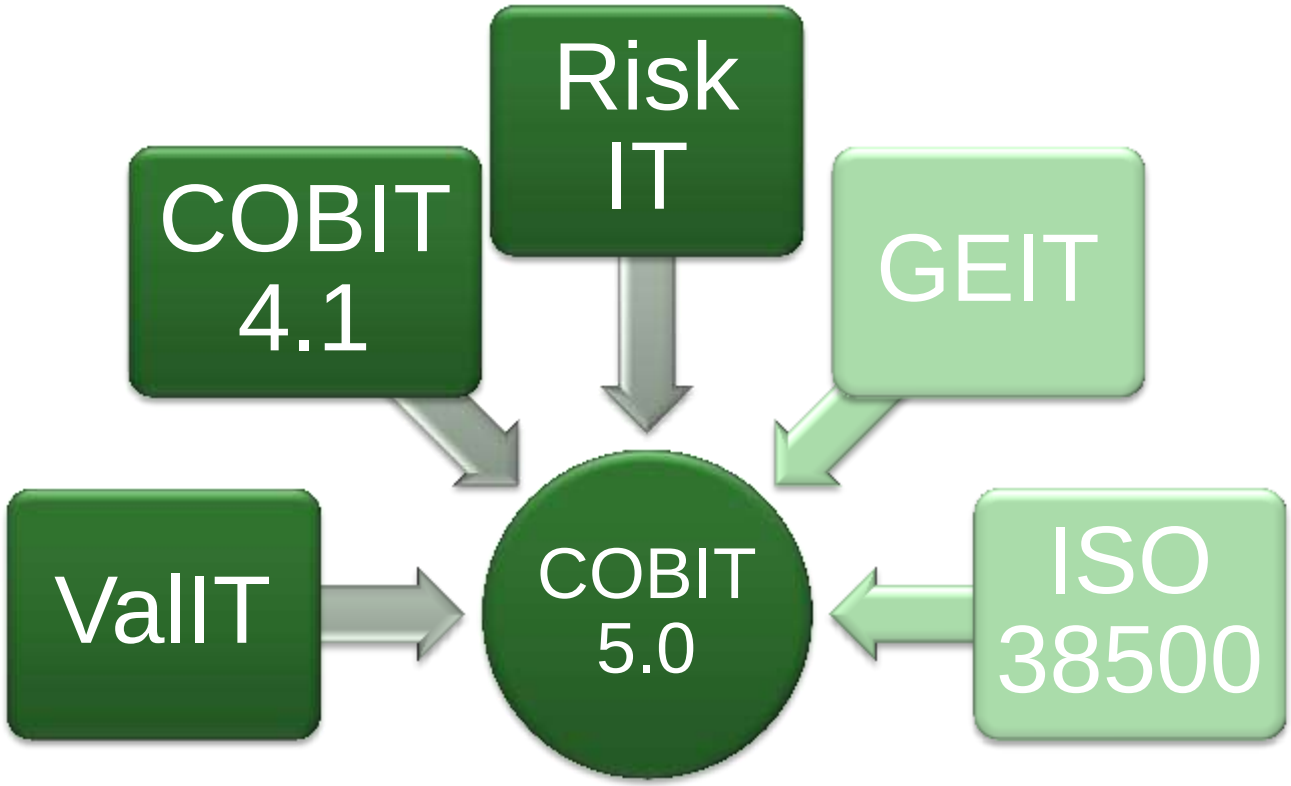


Evolución COBIT



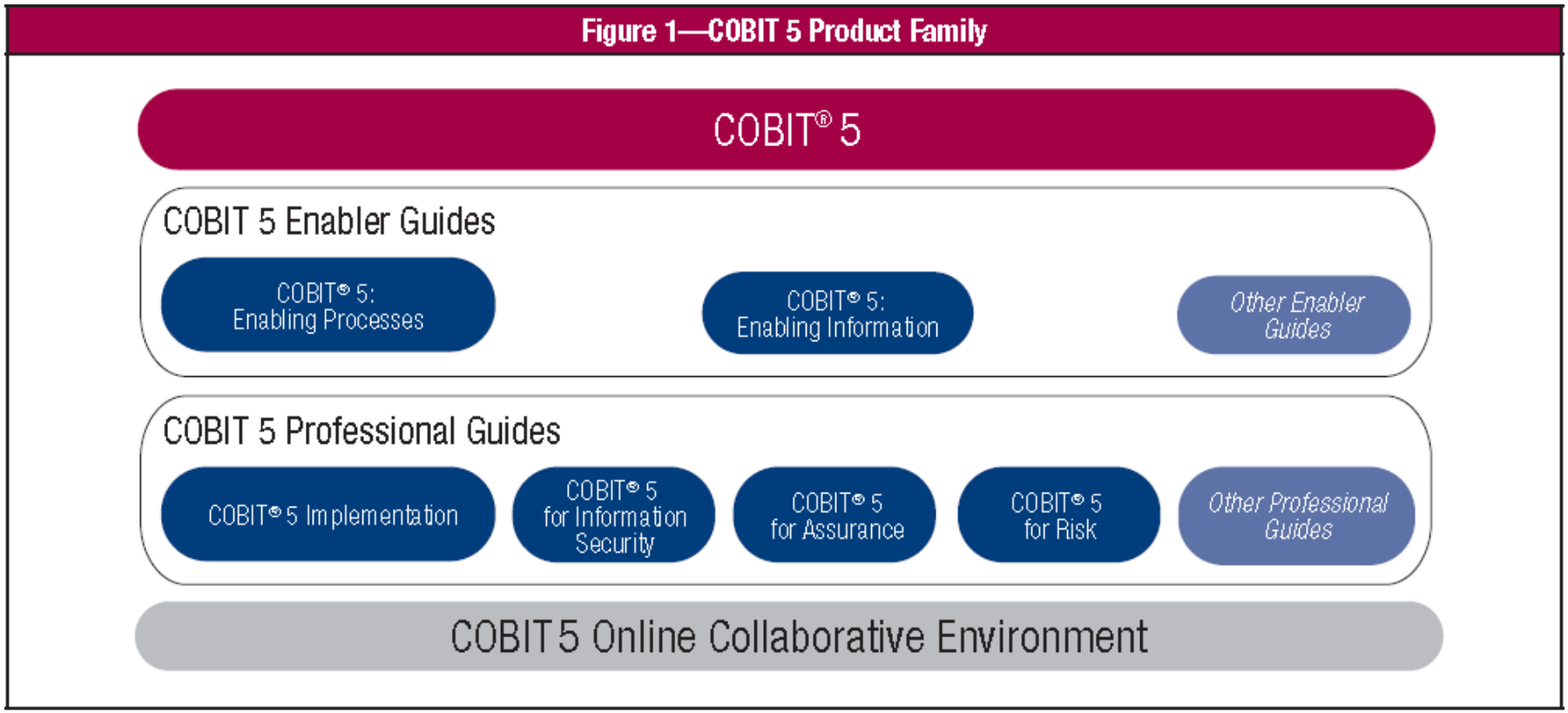
An business framework from ISACA, at www.isaca.org/cobit

Evolución COBIT



ISO 38500: IT Governance Standard
GEIT: de ITGI (IT Governance Intitution)
Val IT marco de trabajo para el gobierno de las inversiones en TI (ITGI)
RiskIT: marco de trabajo para la gestión de riesgo de negocio relacionados con TI

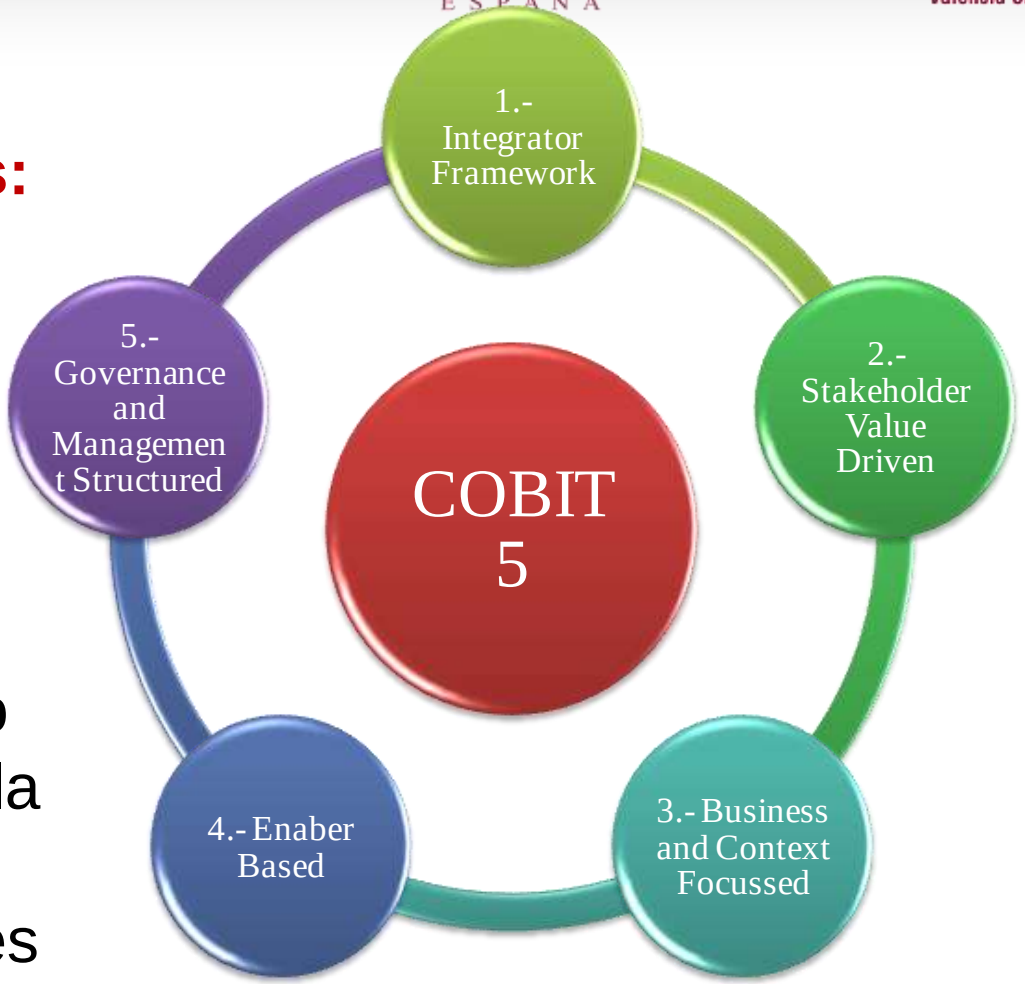
Evolución COBIT



Principios

Basado en 5 principios:

1. Un único marco integrador (y gratuito).
2. Conductores que crean valor para los interesados.
3. Foco sobre el negocio y su contexto para toda la organización
4. Basado en facilitadores
5. Diferenciación entre Gobierno y Gestión



Principios

•Aplicar un único marco de trabajo integrado.

COBIT cubre todas las necesidades y se integra con otros marcos y buenas prácticas, de forma que puede ser utilizado como marco general.

• Satisfacer las necesidades de los Stakeholders (Interesados)

Crear valor manteniendo el equilibrio entre realización de beneficios y la optimización del uso de recursos y gestión del riesgo.

• Cubrir la organización de principio a fin.

Integrando el Gobierno corporativo con el Gobierno de las TI.
Orientación al negocio.

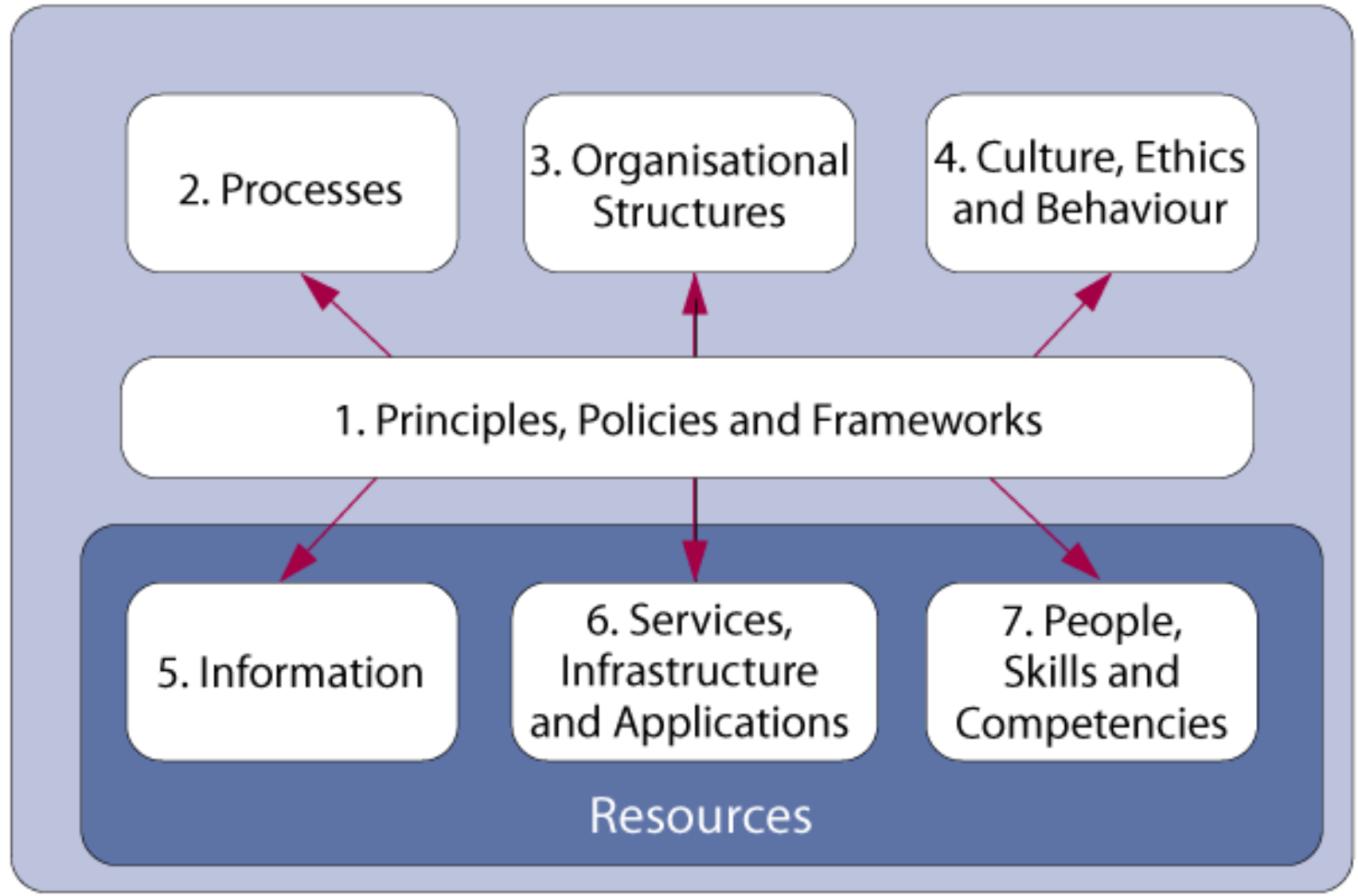
• Aproximación holística (enfoque de negocio).

Para conseguir una Gestión y Gobierno de las TI con eficiencia y eficacia.

•Separar *Gestión* de *Gobierno*.

Ambas disciplinas son importantes y complementarias.

Facilitadores



Facilitadores

Dirigido por 7 facilitadores:

1.- Principios, políticas y marcos

Son los vehículos para trasladar el comportamiento deseado en una guía práctica para conducir las tareas de gestión TI en el día a día.

2.- Procesos

Constituyen un conjunto organizado de prácticas y actividades para conseguir alcanzar los objetivos establecidos respecto a las tecnologías de la información.

3.- Estructura organizacional

Son las entidades de la organización que toman las decisiones críticas.




4.- Cultura, Ética y Comportamiento

Tanto de los individuos como de la organización. Muy a menudo se subestima su influencia en la consecución de los objetivos de Gobierno establecidos.

5.- Información.

La información invade todos los ámbitos de la organización. Es necesitada por esta para operar y para la toma de decisiones. También puede ser el resultado de la actividad de la organización.

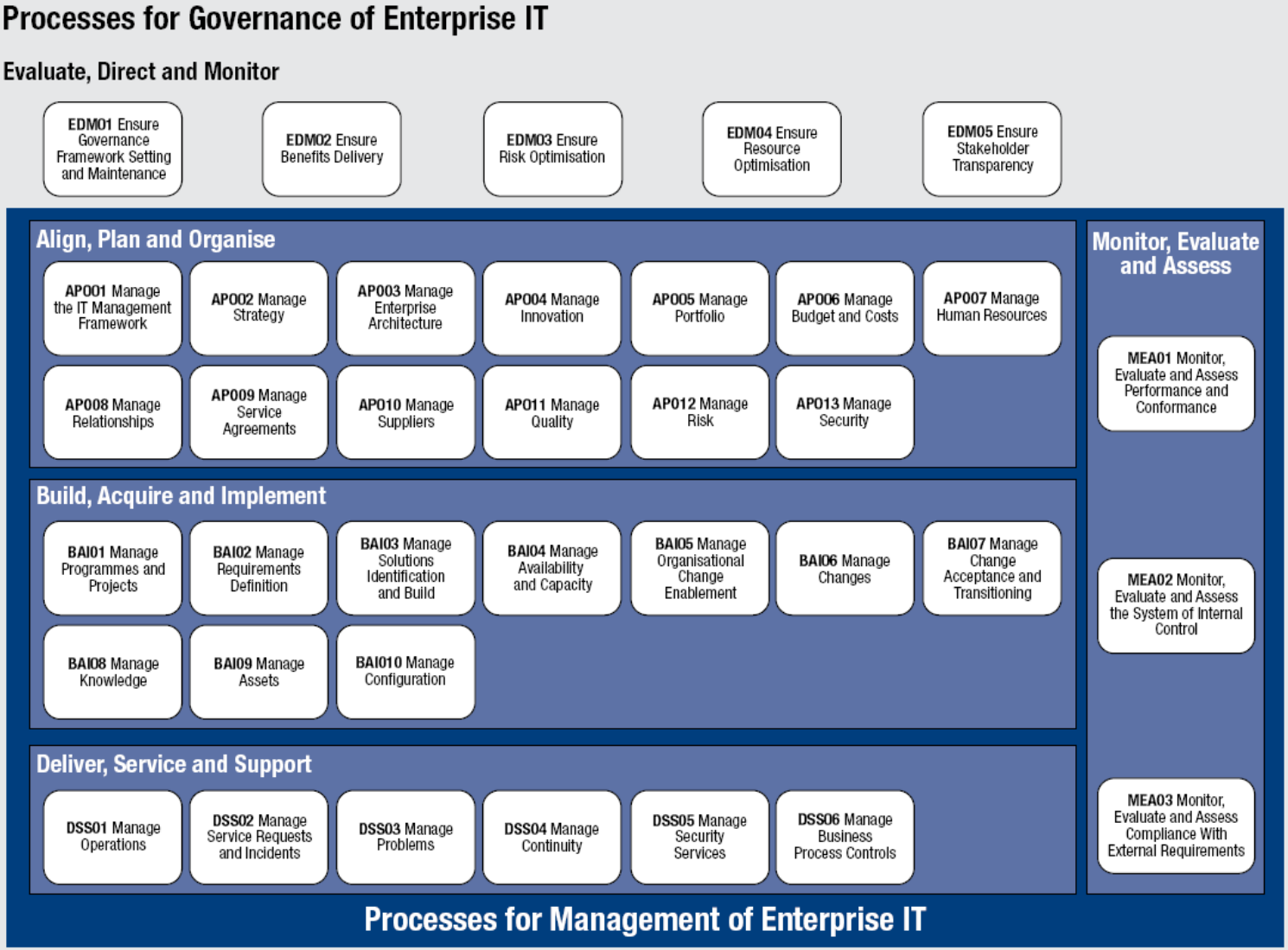
6.- Servicios, Infraestructura y Aplicaciones

Es la parte más cercana a los profesionales de las TIC.

7.- Personas, habilidades y competencias

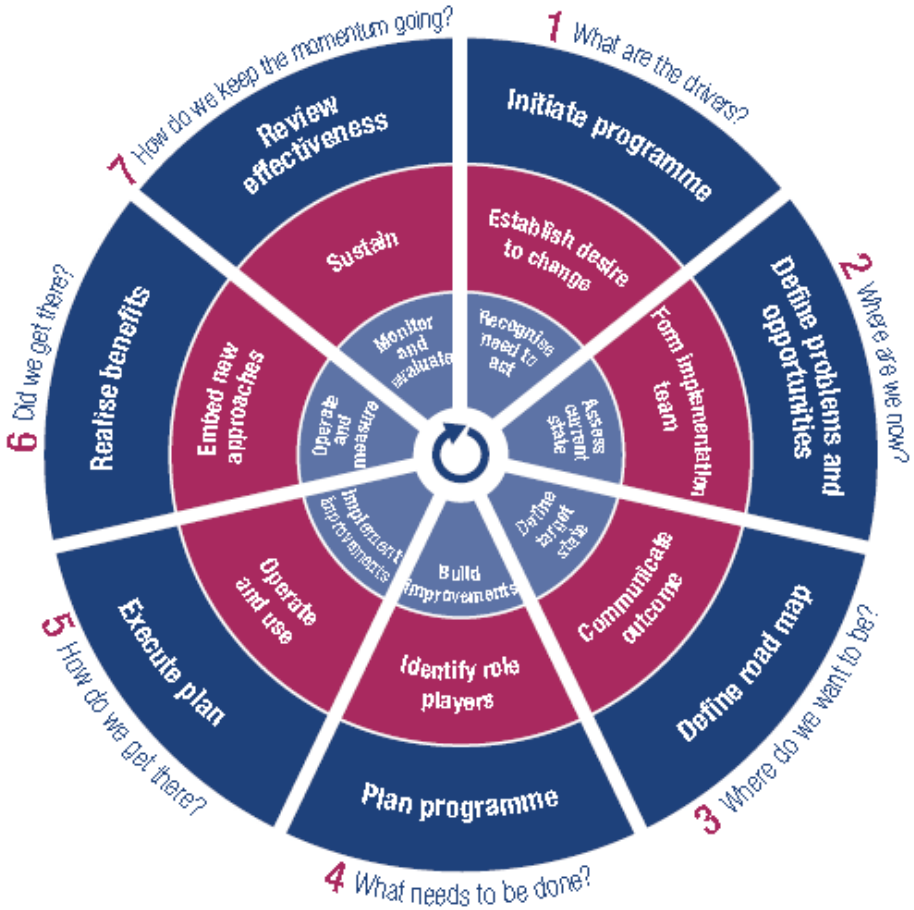
Se asocia a las personas necesarias para realizar las actividades, tomar decisiones y realizar tareas correctivas**.**

Procesos de Gobierno y Gestión (37)



Implementación

Figure 17—The Seven Phases of the Implementation Life Cycle



- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

Implementación

Comité de la Comunidad Valenciana itSMF ESPAÑA

ISACA Valencia Chapter

Figure 16—Roles in Phase 1	
When you are...	Your role in this phase is to...
Board and executive	Provide guidance regarding stakeholder needs, business strategy, priorities, objectives and guiding principles with respect to governance and management of enterprise IT. Approve the high-level approach.
Business management	Together with IT, ensure that stakeholder needs and business objectives have been stated with sufficient clarity to enable translation into business goals for IT, and provide input to understanding of risk and priorities.
IT management	Gather requirements and objectives from all stakeholders, gaining consensus on approach and scope. Provide expert advice and guidance regarding IT matters.
Internal audit	Provide advice and challenge proposed activities and actions, ensuring that objective and balanced decisions are made.
R	

Figure 17—Phase 1 Description	
Phase 1	What Are the Drivers?
Phase objective	Obtain an understanding of the programme background and objectives and current governance approach. Define the initial programme concept business case. Obtain the buy-in and commitment of all key stakeholders.
Phase description	This phase articulates the compelling reasons to act within the organisational context. In this context the programme background, objectives and current governance culture are defined. The initial programme concept business case is defined. The buy-in and commitment of all key stakeholders is obtained.
Continual improvement (CI) tasks	Recognise the need to act: 1. Identify current governance context, business IT and IT pain points, events and symptoms triggering the need to act. 2. Identify the business and governance drivers and compliance requirements for improving GEIT and assess current stakeholder needs. 3. Identify business priorities and business strategy dependent on IT, including any current significant projects. 4. Align with enterprise policies, strategies, guiding principles and any ongoing governance initiatives. 5. Raise executive awareness of IT's importance to the enterprise and the value of GEIT. 6. Define GEIT policy, objectives, guiding principles and high-level improvement targets. 7. Ensure that the executives and board understand and approve the high-level approach and accept the risk of not taking any action on significant issues.

Implementación

Comité de la Comunidad Valenciana itSMF ESPAÑA

ISACA Valencia Chapter

Figure 17—Phase 1 Description *(cont.)*

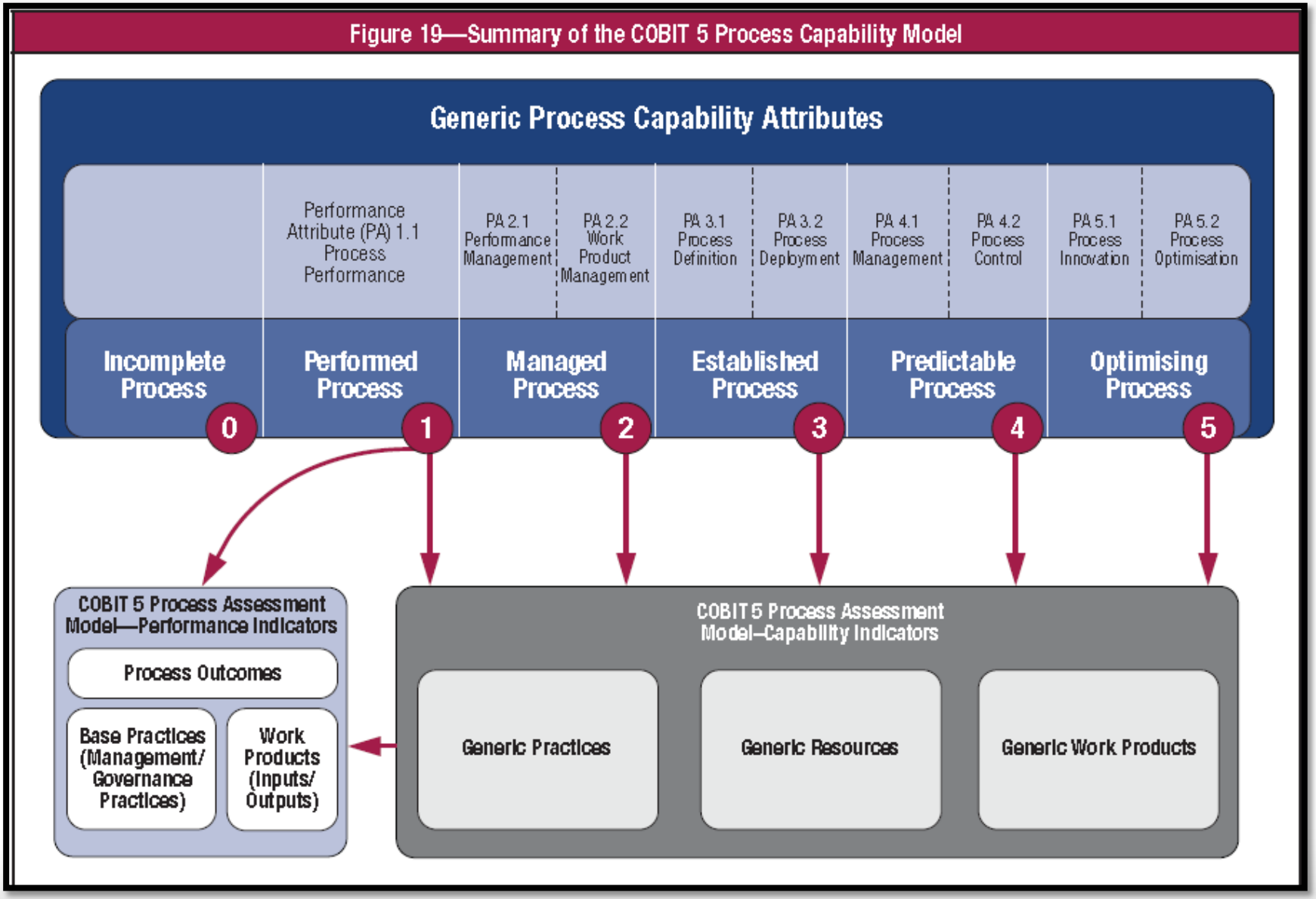
Phase 1	What Are the Drivers?
ISACA materials and other frameworks	• COBIT 5 (enterprise goals, enablers) • *COBIT 5: Enabling Processes* (EDM01; AP001; MEA01), *www.isaca.org/cobit* • *COBIT 5 Implementation* (appendices A. Mapping Pain Points to COBIT 5 Processes, B. Example Decision Matrix and D. Example Business Case) • ISACA supporting products as currently defined at *www.isaca.org* • *The Business Case Guide: Using Val IT 2.0*
Output	• Business case outline • High-level roles and responsibilities • Identified stakeholder map, including support and involvement required, influence and impact, and agreed-on

Figure 18—Phase 1 RACI Chart

Key Activities	Responsibilities of Implementation Role Players: Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
Identify issues triggering need to act (CI1).	C/I	A	R	R	C	C	C	C	R
Identify business priorities and strategies affecting IT (CI3).	C	A	R	R	C	C	C	C	R
Gain management agreement to act and obtain executive sponsorship (CI7).	C	A/R	R	C	I	I	I	I	R
Instil the appropriate level of urgency to change (CE10).	I	A	R	R	C	C	C	C	R
Produce convincing outline business case (PM3).	I	A	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Implementación



Se busca …

… experto en hacer NUDOS DE CORBATA

Cómo hacer nudos de corbata ¿Qué me pongo hoy?

Jaume Siscar Bondia
CISA, CISM, CGEIT, CRISC, LA ISO 27000
Director de Certificaciones ISACA Valencia