Monterrey Chapter

Evento Técnico 3 de Mayo de 2012

Conferencista:

José Ángel Peña Ibarra, CGEIT, CRISC

japi@ccisa.com.mx

Contenido

I. Introducción
II. Marco de referencia COBIT 5
III. Procesos habilitadores
IV. Guía de Implementación
V. Diferencias de COBIT 5 con COBIT 4.1
VI. Futuros productos COBIT

japi@ccisa.com.mx

I. Introducción

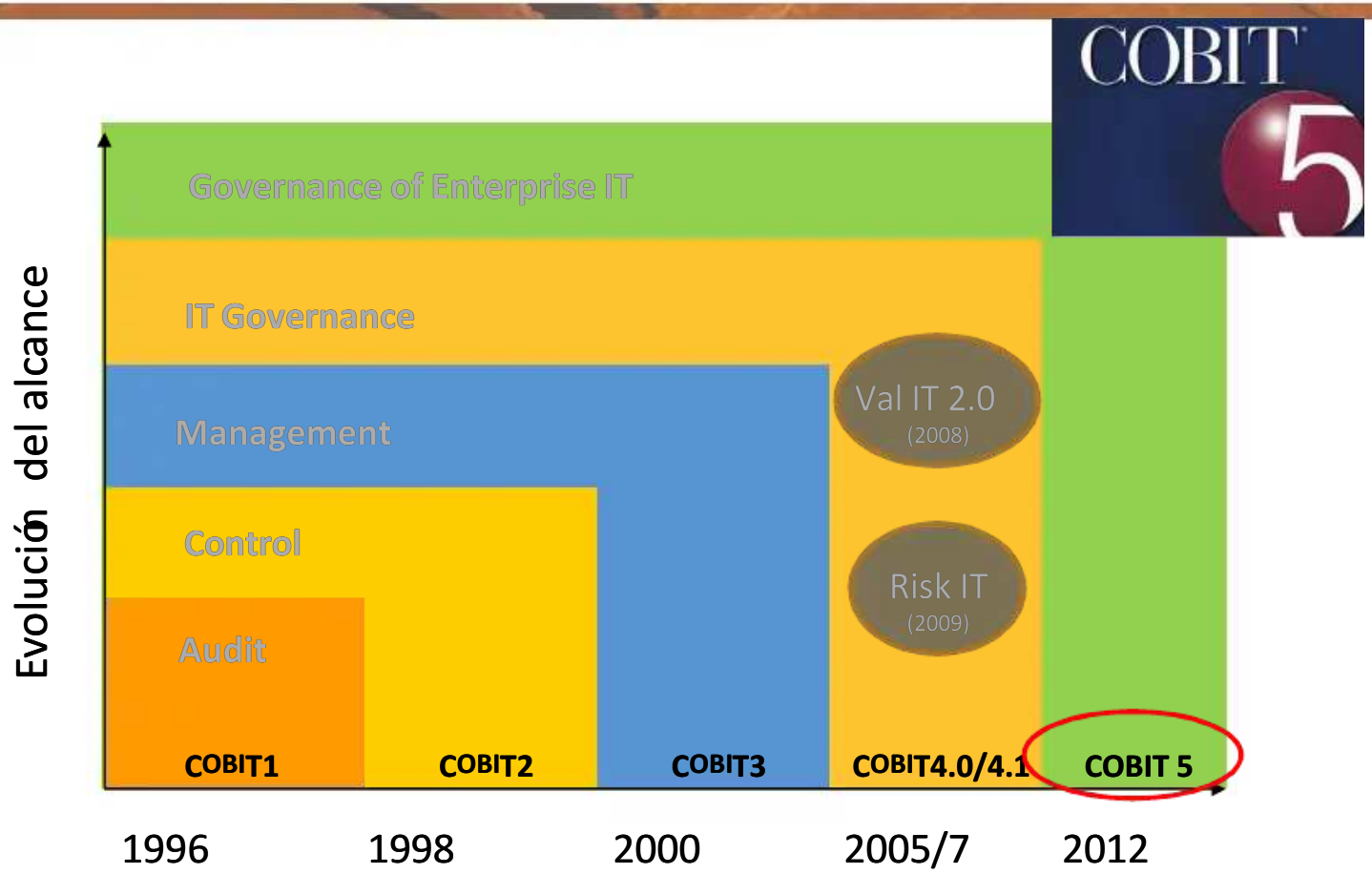
japi@ccisa.com.mx

COBIT 5 ya está aquí

- El 9 de abril de 2012 fue publicado oficialmente por ISACA el marco de referencia COBIT 5.
- Es la evolución de la familia COBIT, aprovechando las versiones anteriores y las practicas actuales.
- Está apoyado en más de 15 años de experiencia global.
- Es resultado del trabajo de expertos de los 5 continentes y de la retroalimentación de cientos de miembros de ISACA.

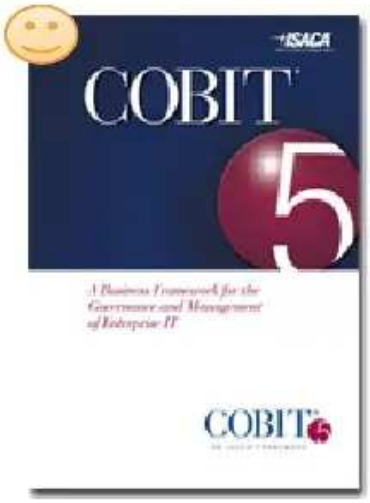
japi@ccisa.com.mx

Evolución de COBIT



Marco de referencia de ISACA, ver en www.isaca.org/cobit

japi@ccisa.com.mx



COBIT 5

COBIT 5 is the overarching business and management framework for governance and management of enterprise IT.

This volume documents the 5 principles of COBIT 5 and defines the 7 supporting enablers that form the framework.

Available 10 April 2012

Members Reserve Today | Join Now and Reserve Your Copy

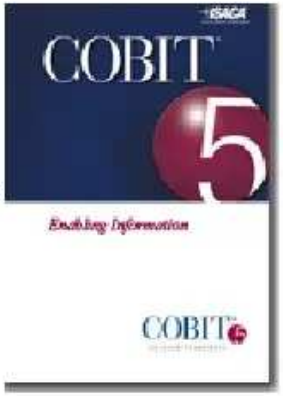
COBIT 5 Enabler Guides

These guides each provide details on specific COBIT 5 governance and management enablers.

COBIT 5: Enabling Processes

A detailed reference guide to the processes defined in the COBIT 5 process reference model. This includes the COBIT 5 goals cascade, a process model explanation and the process reference model.

Available 10 April 2012



COBIT 5: Enabling Information

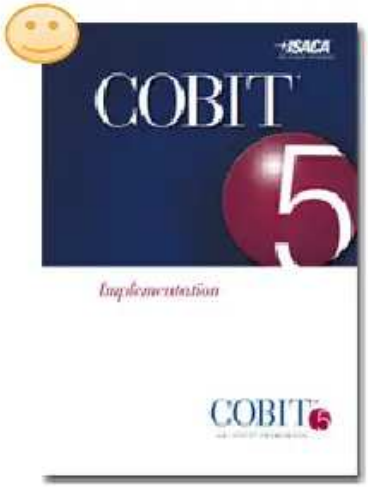
A detailed reference guide to the Information enablers defined in COBIT 5. This volume will extend the Information enabler guidance to provide more detailed, practical guidance on the governance and management of enterprise information assets.

In Planning

Familia de productos COBIT 5

COBIT 5 Professional Guides

These guides each provide COBIT 5 guidance for a particular type of professional user.

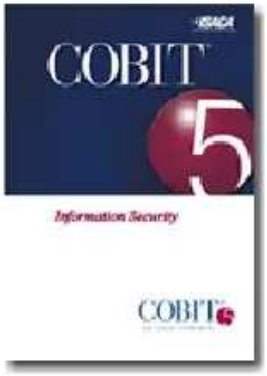


COBIT 5 Implementation

A good-practice approach for implementing governance of enterprise IT (GEIT) based on a continual improvement life cycle that should be tailored to suit the enterprise's specific needs.

Available 10 April 2012

Members Reserve Today | Join Now and Reserve Your Copy



COBIT 5 for Information Security

This publication expands on the COBIT 5 framework content by providing more detail and more practical guidance on how information security professionals can use COBIT in delivering their products and services.

Available July 2012

COBIT 5 for Assurance

This publication expands on the COBIT 5 framework content by providing more detail and practical guidance on how information assurance professionals can use COBIT in delivering products and services.

In Planning

El marco COBIT 5

- COBIT 5 ayuda a las empresas a crear/obtener valor óptimo de la TI, manteniendo un balance entre los beneficios, riesgos y recursos.
- COBIT 5 tiene un **enfoque holístico** para administrar y gobernar la información y tecnología relacionada en toda la empresa,
- COBIT 5 establece **principios** y **habilitadores** genéricos que son útiles para empresas de todos tamaños y giros.

Gobierno y Administración

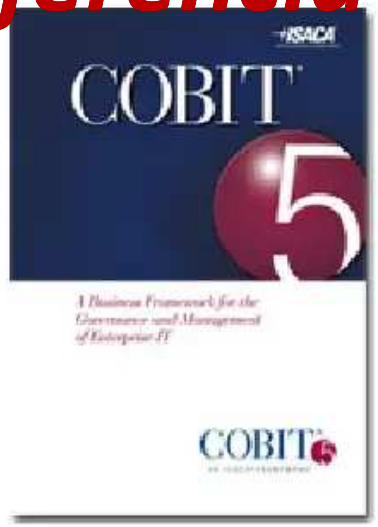
- **El Gobierno o Gobernanza** se asegura de que los objetivos de la empresa son logrados, **evaluando** las necesidades de los interesados, condiciones y opciones; estableciendo la **dirección** mediante prioridades y toma de decisiones; y **monitoreando** el desempeño, cumplimiento y progreso respecto a los objetivos **(EDM).**

- **La Administración planea, construye, ejecuta y monitorea (plans, builds, runs** and **monitors)** actividades en alineamiento con la dirección establecida por el cuerpo de gobierno para alcanzar los objetivos de la empresa **(PBRM).**

En resumen …

- **COBIT 5** está enfocado en el **Gobierno Empresarial de la TI.**
- Se fundamenta en **5 principios** que permiten a la empresa construir un efectivo marco de **gobierno y administración de TI.**
- Se basa en un conjunto holístico de **7 habilitadores**.
- Considera las tendencias actuales de gobierno y administración y está **alineado con otros marcos de referencia**.
- Establece un nuevo **Modelo de Referencia de Procesos de TI**

II. COBIT 5 Marco de Referencia



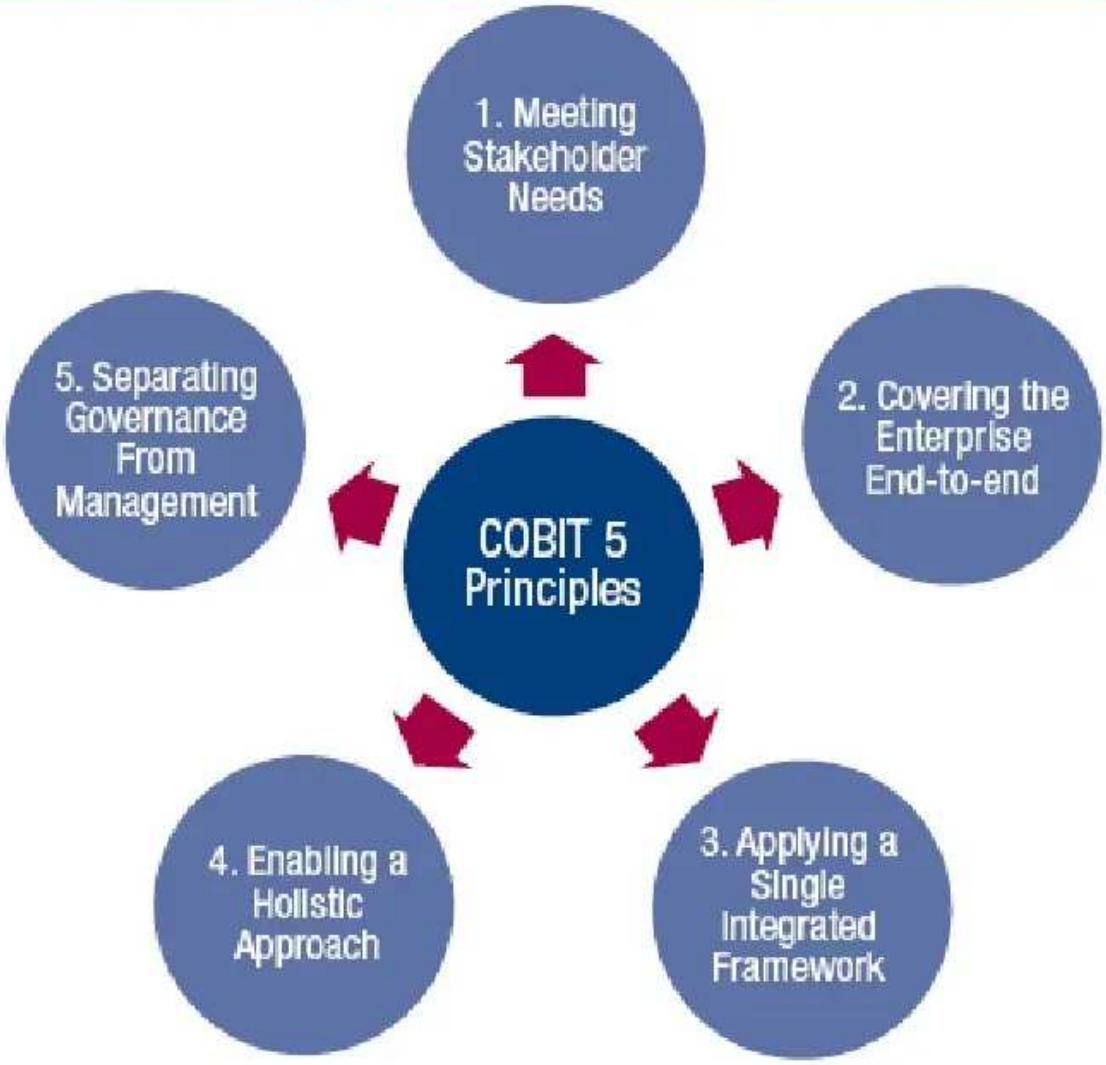
japi@ccisa.com.mx

Marco de referencia COBIT 5

COBIT 5:

- Es el principal producto, que cubre (*overarching*) a los demás de la familia COBIT 5.
- Contiene el resumen ejecutivo y la descripción completa de los componentes del marco COBIT 5:
  - **Los 5 principios de COBIT 5**
  - **Los 7 habilitadores de COBIT 5** y
  - Una introducción a la guía de implementación de COBIT 5
  - Una introducción al COBIT Assessment Programme (no especifico a COBIT 5)

Principios de COBIT 5



japi@ccisa.com.mx

Principios de COBIT 5

Los cinco principios de COBIT 5:

1. Satisfacer las necesidades de los interesados
2. Cubrir la empresa de extremo a extremo
3. Aplicar un solo marco integrado
4. Habilitar un enfoque Holístico
5. Separar Gobierno de Administración

1. Satisfacer las necesidades de los interesados

Principio 1. Satisfacer las necesidades de los interesados

- Empresas existen para **crear valor** para sus interesados

1. Satisfacer las necesidades de los interesados (cont.)

Principio 1. Satisfacer las necesidades de los interesados:

- Las Empresas tienen **muchos** interesados, y **"crear valor"** significa diferentes y a veces contrarias cosas a cada uno.
- Gobernar es acerca de negociar y decidir entre los diferentes interesados.
- El sistema de gobierno debe considerar a todos los interesados .
- Para cada decisión, se debe preguntar:
  - ¿Quién recibe los beneficios?
  - ¿ A quién impacta el riesgo?
  - ¿ Qué recursos se necesitan?

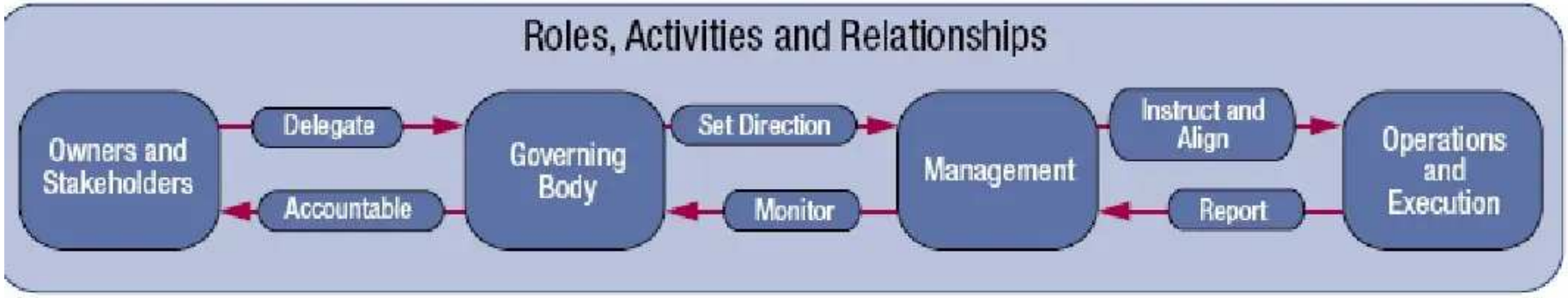
2. Cubrir la empresa de extremo a extremo

Principio 2. Cubrir la empresa de extremo a extremo:

- Esto significa que COBIT 5:
  - Integra el gobierno empresarial de TI en el gobierno corporativo..
  - Cubre todas las funciones y procesos dentro de la empresa; ***(COBIT 5 does not focus only on the 'IT function').***

2. Cubrir la empresa de extremo a extremo (cont.)

Principio 2. Cubrir la empresa de extremo a extremo:



japi@ccisa.com.mx

3. Aplicar un solo marco integrado

Principio 3. Aplicar un solo marco integrado:

- COBIT 5 se alinea con los estándares y marcos más relevantes usados por las empresas:
  - Empresariales: COSO, COSO ERM, ISO/IEC 9000,
  - Relacionados con TI: ISO/IEC 38500, ITIL, serie ISO/IEC 27000, TOGAF,
  - Etc.
- Esto permite que la empresa use COBIT 5 como un marco integrador de gobierno y administración de TI.

4. Habilitar un enfoque Holístico

Principio 4. Habilitar un enfoque Holístico

Los habilitadores de COBIT 5 son:

- Factores que, individual y colectivamente influencian para que algo funcione. En el caso de COBIT, este algo, son el gobierno y la administración de TI empresarial.
- Se describen los habilitadores de COBIT 5 en **siete categorías.**

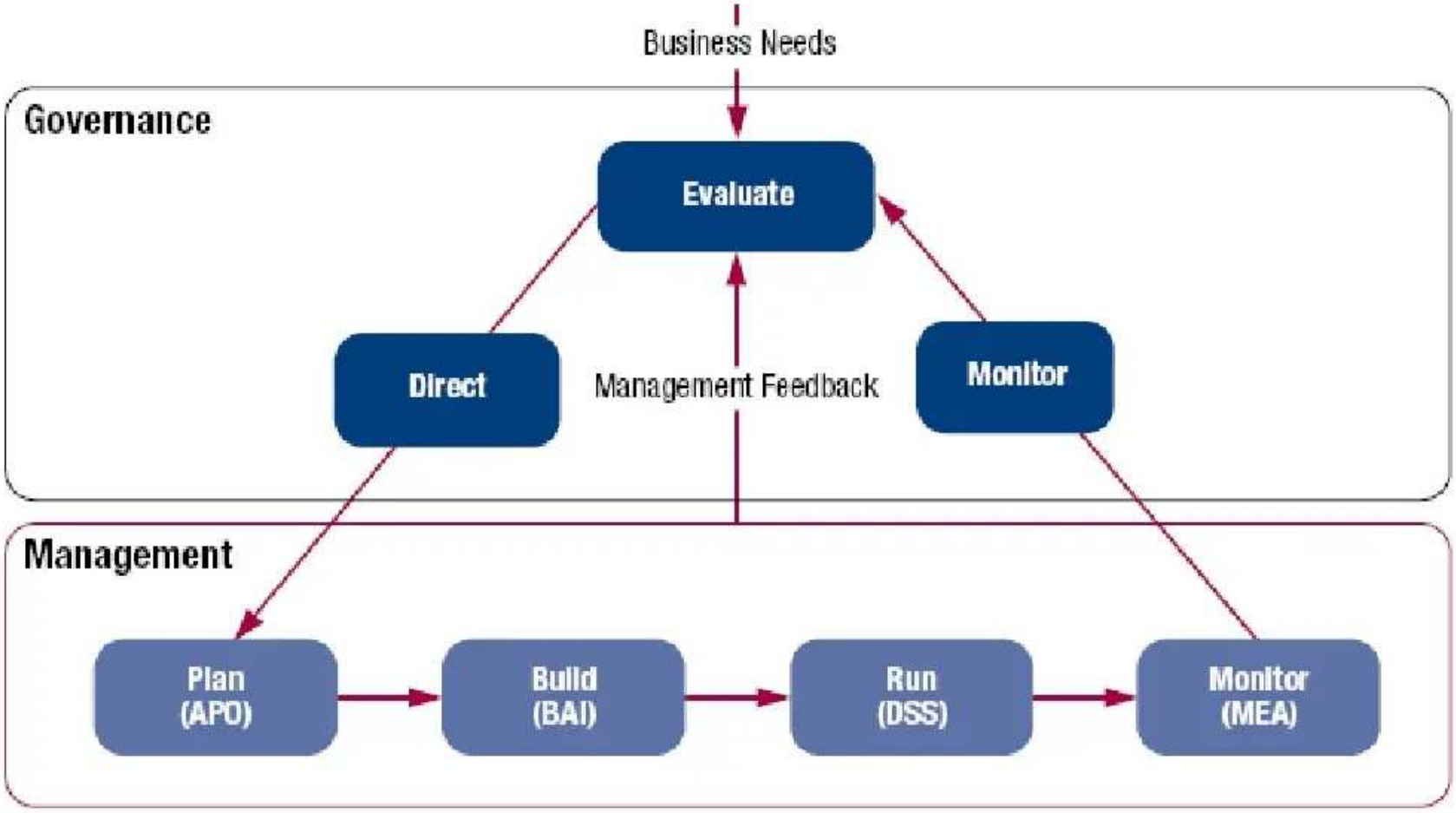
5. Separar Gobierno de Administración

Principio 5. Separar Gobierno de Administración:

- Estas dos disciplinas:
  - Incluyen diferentes tipos de actividades
  - Requieren diferentes estructuras organizacionales
  - Sirven para diferentes propósitos
- **Gobierno—** Responsabilidad de la Junta Directiva.
- **Administración—**Responsabilidad de la alta administración, bajo el liderazgo del CEO.

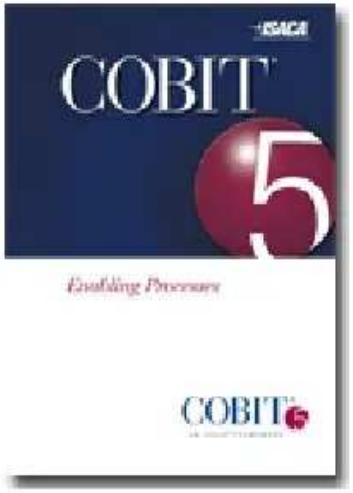
japi@ccisa.com.mx

5. Separar Gobierno de Administración



japi@ccisa.com.mx

III. COBIT 5: Enabling Processes

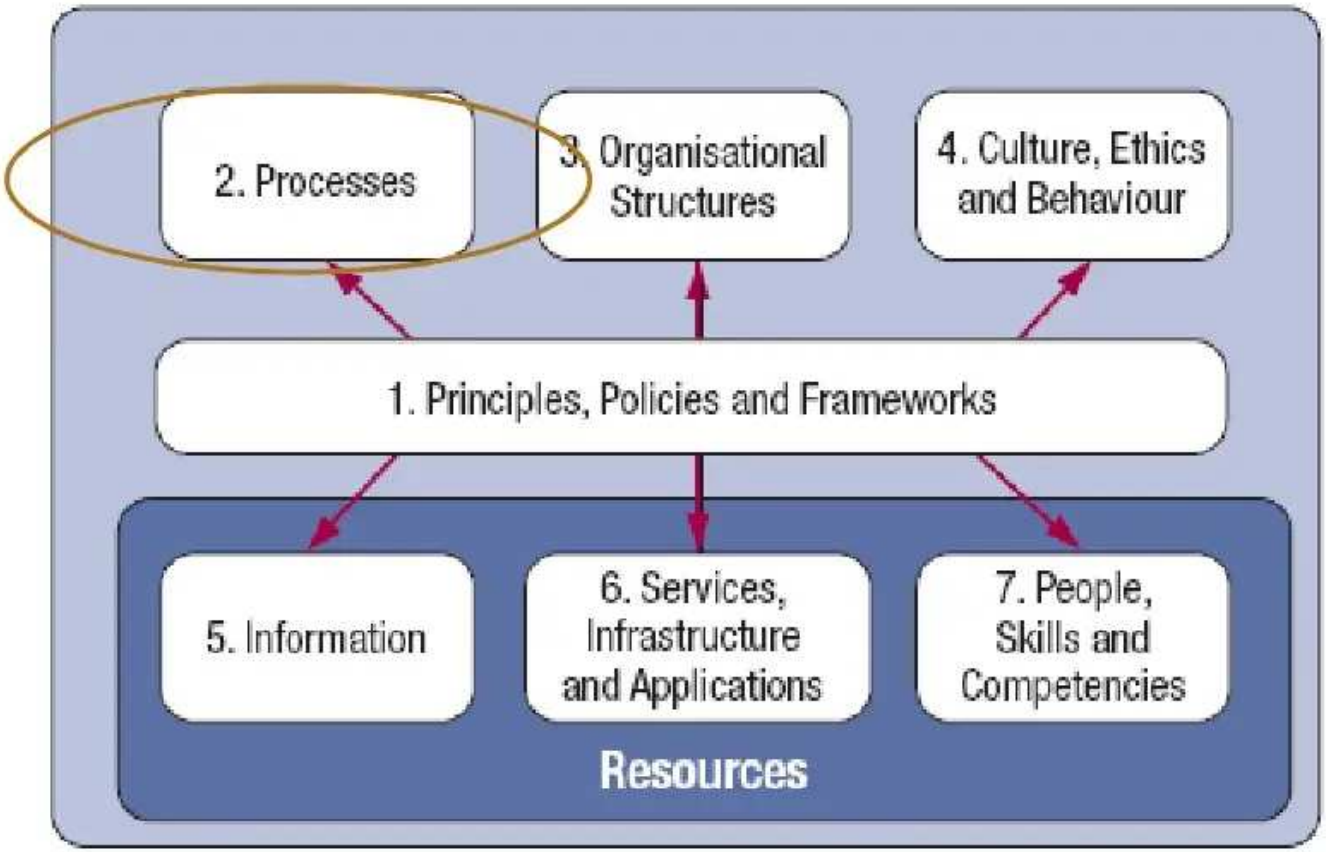


japi@ccisa.com.mx

COBIT 5: Procesos Habilitadores

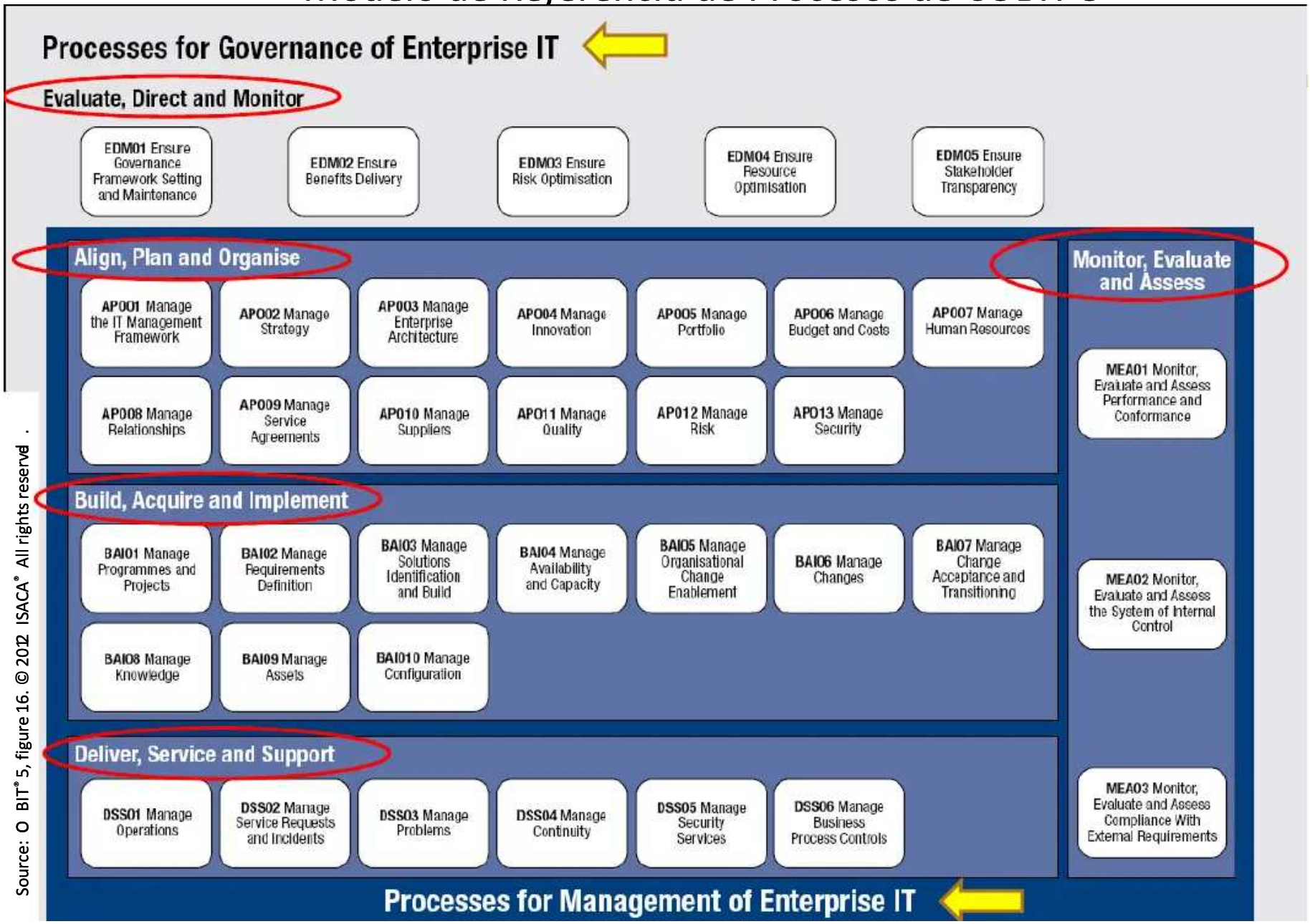
- *COBIT 5: Enabling Processes* complementa el marco COBIT 5 y contiene una guía de referencia detallada a los procesos que están definidos en el Modelo de referencia de Procesos de COBIT 5:
  - El Capítulo 4 muestra el diagrama del modelo de referencia de procesos.
  - El Capítulo 5 contiene la información detallada de los 37 procesos de COBIT 5.

COBIT 5 Enablers



japi@ccisa.com.mx

Modelo de Referencia de Procesos de COBIT 5



COBIT 5: Procesos Habilitadores (cont).

- En *COBIT 5: Enabling Processes* cada uno de los 37 procesos contiene prácticas de gobierno o prácticas de administración (según sea proceso de gobierno (EDM) o proceso de Administración (APO, BAI, DSS y MEA)
- Las prácticas a sus vez contienen actividades
- Se presenta una *RACI chart*, que es más detallada que la de COBIT 4.1
- Al principio de cada dominio se listan los procesos que engloba.

Build, Acquire and Implement (BAI)

01 Manage programmes and projects.

02 Manage requirements definition.

03 Manage solutions identification and build.

04 Manage availability and capacity.

05 Manage organisational change enablement.

06 Manage changes.

07 Manage change acceptance and transitioning.

08 Manage knowledge.

09 Manage assets.

10 Manage configuration.

BAI06 Manage Changes	Area: Management Domain: Build, Acquire and Implement

Process Description
Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.

Process Purpose Statement
Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

The process supports the achievement of a set of primary IT-related goals:

IT-related Goal	Related Metrics
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines

Process Goals and Metrics

Process Goal	Related Metrics

Process Goals and Metrics

Process Goal	Related Metrics
1. Authorised changes are made in a timely manner and with minimal errors.	• Amount of rework caused by failed changes • Reduced time and effort required to make changes • Number and age of backlogged change requests
2. Impact assessments reveal the effect of the change on all affected components.	• Percent of unsuccessful changes due to inadequate impact assessments
3. All emergency changes are reviewed and authorised after the change.	• Percent of total changes that are emergency fixes • Number of emergency changes not authorised after the change
4. Key stakeholders are kept informed of all aspects of the change.	• Stakeholder feedback ratings on satisfaction with communications

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		

2. Impact assessments reveal the effect of the change on all affected components.	• Percent of unsuccessful changes due to inadequate impact assessments
3. All emergency changes are reviewed and authorised after the change.	• Percent of total changes that are emergency fixes • Number of emergency changes not authorised after the change
4. Key stakeholders are kept informed of all aspects of the change.	• Stakeholder feedback ratings on satisfaction with communications

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

v1PUC55.pdf - Adobe Reader

uda

150 / 230 125% Herr

BAI06 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI06.01 Evaluate, prioritise and authorise change requests. Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.	BAI03.05	Integrated and configured solution components	Impact assessments	Internal
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors		
	DSS03.05	Identified sustainable solutions	Change plan and schedule	BAI07.01
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		

Activities

1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.
2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.
3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.
4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.
5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.

rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.	BAI03.09	Record of all approved and applied change requests	Change request status reports	BAI01.06 BAI10.03

Activities

1. Categorise change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.
4. Maintain a tracking and reporting system for all change requests.

Management Practice	Inputs		Outputs	
BAI06.04 Close and document the changes. Whenever changes are implemented, update accordingly the solution and user documentation and the procedures affected by the change.	**From**	**Description**	**Description**	**To**
			Change documentation	Internal

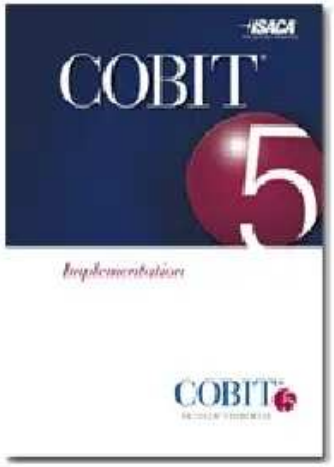
Activities

1. Include changes to documentation (e.g., business and IT operational procedures, business continuity and disaster recovery documentation, configuration information, application documentation, help screens, and training materials) within the change management procedure as an integral part of the change.
2. Define an appropriate retention period for change documentation and pre- and post-change system and user documentation.
3. Subject documentation to the same level of review as the actual change.

BAI06 Related Guidance

Related Standard	Detailed Reference
ISO/IEC 20000	9.2 Change management
ITIL V3 2011	13. Change Management

IV. COBIT 5 Implementation

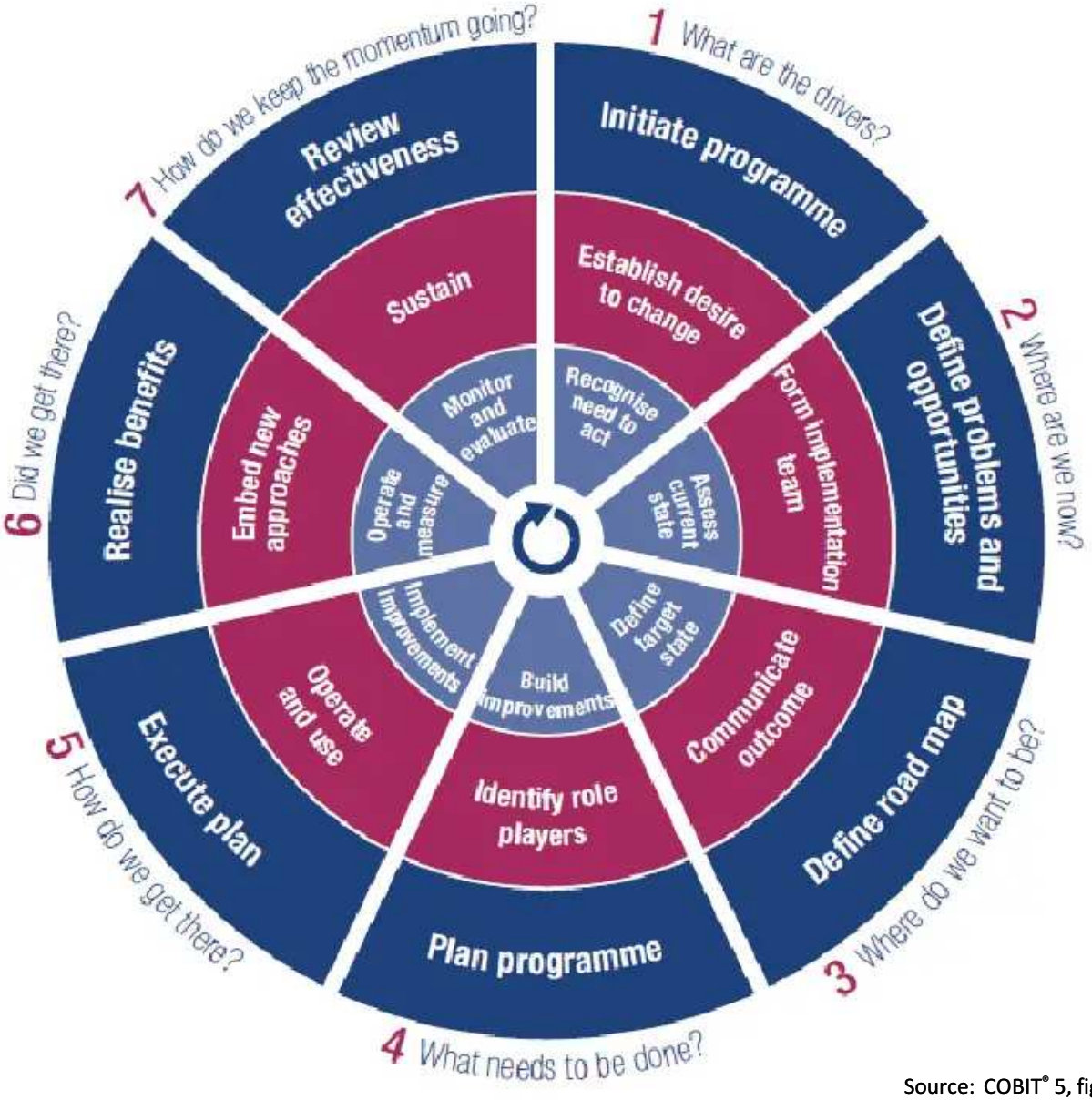


japi@ccisa.com.mx

COBIT 5 Implementación

- *COBIT 5: Implementation* cubre lo siguiente:
  - Posicionar GEIT (Governance of Enterprise IT) dentro de la empresa
  - Dar los primeros pasos hacia el mejoramiento del GEIT
  - Retos de Implementación y Factores de Éxito
  - Habilitar el cambio organizacional y de conducta relacionado con GEIT
  - Mejora Continua

Las 7 fases del ciclo de implementación



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

V. Diferencias de COBIT 5 con COBIT 4.1

japi@ccisa.com.mx

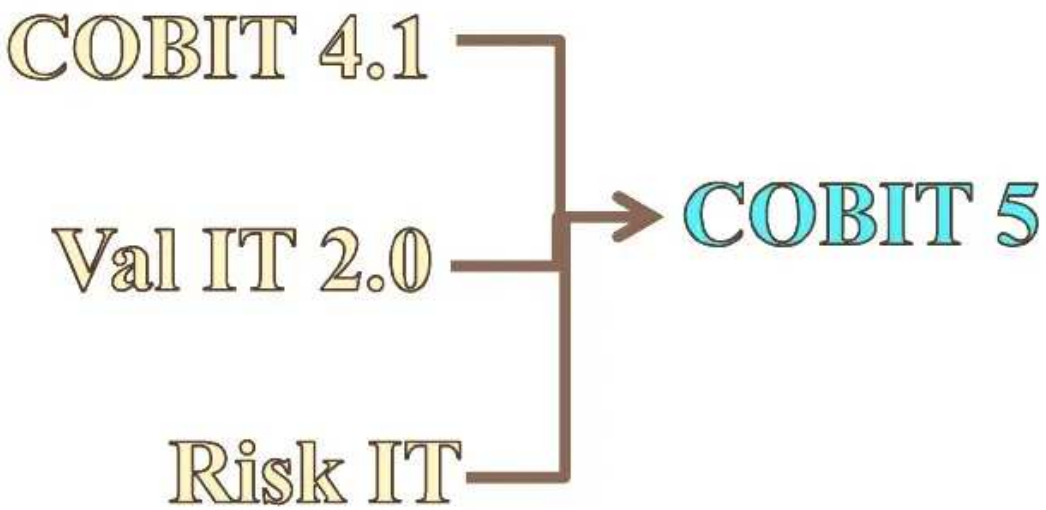
Áreas de cambio

- Los principales cambios en COBIT 5:

1. Nuevos Principios de GEIT
2. Mayor foco en Habilitadores
3. Nuevo Modelo de Referencia de Procesos
4. Nuevos y modificados procesos
5. Prácticas y Actividades
6. Metas y Métricas más desarrolladas
7. Entradas y Salidas a nivel de práctica
8. RACI Charts más detalladas
9. Process Capability Maturity Models and Assessments

Integración de Val IT y Risk IT

- COBIT 5 ha integrado el contenido de COBIT 4.1, Val IT and Risk IT en un Modelo de Referencia de Procesos



Nuevos y modificados procesos

- Hay nuevos y modificados procesos, en particular:
  - APO03 Manage enterprise architecture.
  - APO04 Manage innovation.
  - APO05 Manage portfolio.
  - APO06 Manage budget and costs.
  - APO08 Manage relationships.
  - APO13 Manage security.
  - BAI05 Manage organisational change enablement.
  - BAI08 Manage knowledge.
  - BAI09 Manage assets.
  - DSS05 Manage security service.
  - DSS06 Manage business process controls.

Prácticas y Actividades

- Las **prácticas** de gobierno y de administración de COBIT 5 son equivalentes a los objetivos de control de COBIT 4.1 y los procesos de Val IT y Risk IT.
- Las **actividades** de COBIT 5 son equivalentes a las prácticas de control de COBIT 4.1 y a las prácticas de administración de Val IT y Risk IT.

Process Capability Maturity Models and Assessments

- COBIT 5 descontinúa el *"COBIT 4.1, Val IT and Risk IT CMM-based capability maturity modelling approach"*.
- COBIT 5 será soportado por un nuevo *"process capability assessment approach"* basado en ISO/IEC 15504.
- Ver:

  www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Assessment-Programme.aspx

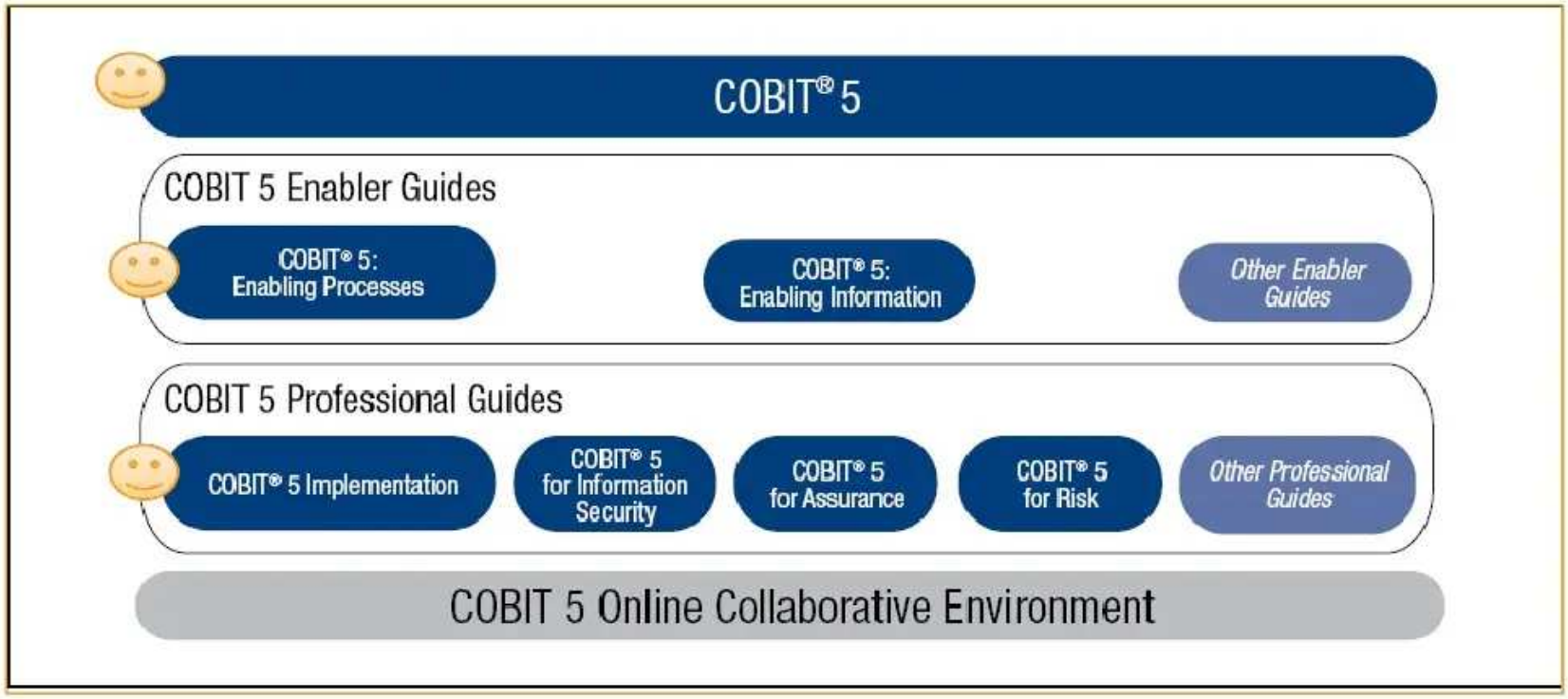
Figure 20—Comparison Table of Maturity Levels (COBIT 4.1) and Process Capability Levels (COBIT 5)

COBIT 4.1 Maturity Model Level	Process Capability Based on ISO/IEC 15504	Context
5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.	**Level 5: Optimising process**—The level 4 predictable process is continuously improved to meet relevant current and projected business goals.	**Enterprise View—Corporate Knowledge**
4 Managed and measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	**Level 4: Predictable process**—The level 3 established process now operates within defined limits to achieve its process outcomes.	
3 Defined process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalisation of existing practices.	**Level 3: Established process**—The level 2 managed process is now implemented using a defined process that is capable of achieving its process outcomes.	
	Level 2: Managed process—The level 1 performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	**Instance View—Individual Knowledge**
2 Repeatable but intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	**Level 1: Performed process**—The implemented process achieves its process purpose. **Remark: It is possible that some classified as Maturity Model 1 will be classified as 15504 0, if the process outcomes are not achieved.**	
1 Initial/*Ad hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.		
0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	**Level 0: Incomplete process**—The process is not implemented or fails to achieve its purpose.	

VI. Futuros productos de la familia COBIT 5

japi@ccisa.com.mx

COBIT 5 Product Family



= Publicados el 9 de abril de 2012

japi@ccisa.com.mx

Monterrey Chapter

Evento Técnico 3 de Mayo de 2012

¡Gracias !

Conferencista:

José Ángel Peña Ibarra, CGEIT, CRISC

japi@ccisa.com.mx