



Para qué sirven los frameworks (modelos) ?

- Manejar complejidad
 - Mejorar Calidad
 - Reducir Riesgos
 - Aumentar el valor que se le ofrece a los usuarios y clientes
 - El uso de frameworks supone que su uso asegura que se tendrán procesos repetibles y que procesos repetibles aumentarán la calidad, reducirán riesgos y permitirán ofrecer más valor a los stakeholders
 - Será siempre el caso?
-

Implementar Gobierno de TI con COBIT

Rubby Casallas

Universidad de los Andes

Qué es Gobernabilidad en TICS?

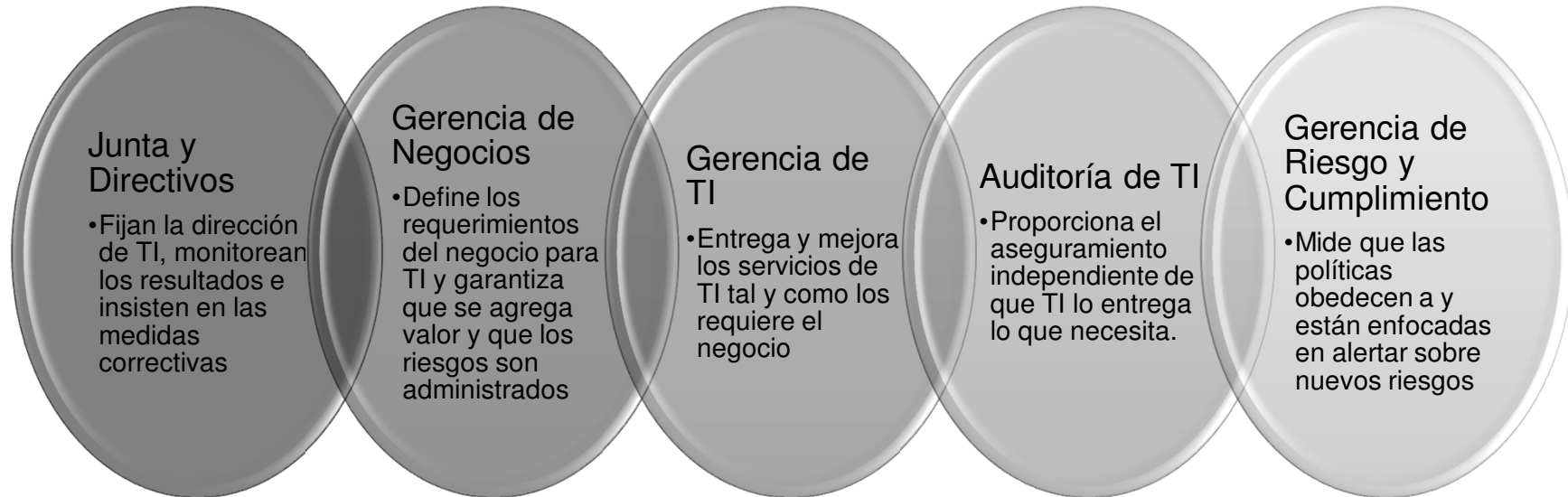
- Es el modelo que se utiliza para garantizar que:
 - Los procesos de gestión de las TICs están alineados con las metas del negocio
 - Las TICs tienen:
 - términos de costos razonables
 - calidad de los servicios
 - oportunidad en la entrega de soluciones
 - mitigación de los riesgos asociados
-

La función de TIC

- Debe:
 - ❑ Entregar valor a la organización (alineación con el negocio)
 - ❑ Con calidad de servicio y oportunidad
 - ❑ Con costos de servicio adecuados
 - ❑ Mitigando los riesgos
-

Implementación del Gobierno de TI utilizando COBIT

Stakeholders en el Gobierno de TI



Principales Áreas del Gobierno de TI



•**Alineación Estratégica** se enfoca en garantizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

•**Entrega de Valor** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

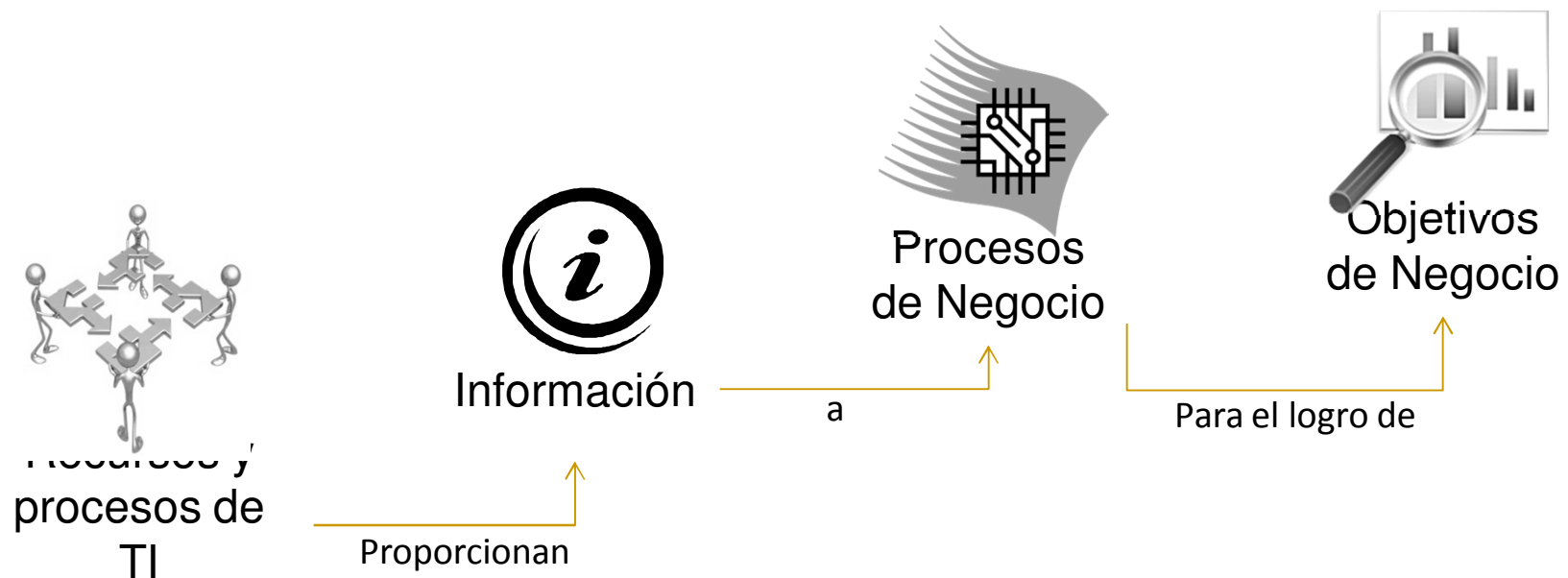
•**Administración de Recursos** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: , aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

•**Administración de Riesgos** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

•**Medición del Desempeño** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

COBIT: Premisa

TI debe entregar la información que una empresa necesita para el logro de sus objetivos.



¿Cómo ayuda COBIT a implementar un Gobierno de TI efectivo?

- Posibilita mapear los objetivos de TI a los objetivos del negocio y viceversa.
 - Mejor alineación, basada en un enfoque del negocio.
 - Una visión comprensible para la administración de lo que es TI.
 - Claridad en la propiedad y responsabilidades, basada en una orientación a procesos.
 - Aceptabilidad general con terceros y reguladores.
 - Entendimiento de los involucrados. Lenguaje común.
-

Por qué COBIT?

- La alta dirección reconoce el impacto significativo que la información puede tener en el éxito de una empresa, por eso espera que TI sea aprovechada con éxito para tener una ventaja competitiva.
 - Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI
-

Por qué COBIT?

- COBIT ofrece un modelo para que las empresas encuentren maneras para:
 - ❑ Alinear la estrategia de TI con la estrategia del negocio
 - ❑ Asegurar que los inversionistas y accionistas logran un debido cuidado estandarizado para la mitigación de los riesgos de TI
 - ❑ Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa
 - ❑ Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas
 - ❑ Crear relaciones constructivas y comunicaciones efectivas entre el negocio y TI, y con socios externos
 - ❑ Medir el desempeño de TI

Ventajas de COBIT

- COBIT esta alineado con otros estándares y buenas practicas y puede usarse en conjunto con ellas.
 - El marco de referencia de COBIT y las mejores practicas que lo soportan proporcionan un ambiente de TI bien administrado y flexible en una organización.
 - COBIT proporciona un ambiente de control que responde a las necesidades del negocio y está al servicio de las funciones de administración y auditoría en términos de sus responsabilidades sobre el control.
 - COBIT proporciona herramientas que ayudan a administrar las actividades de TI.
-

COBIT: Enfocado al Negocio

- Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.
-

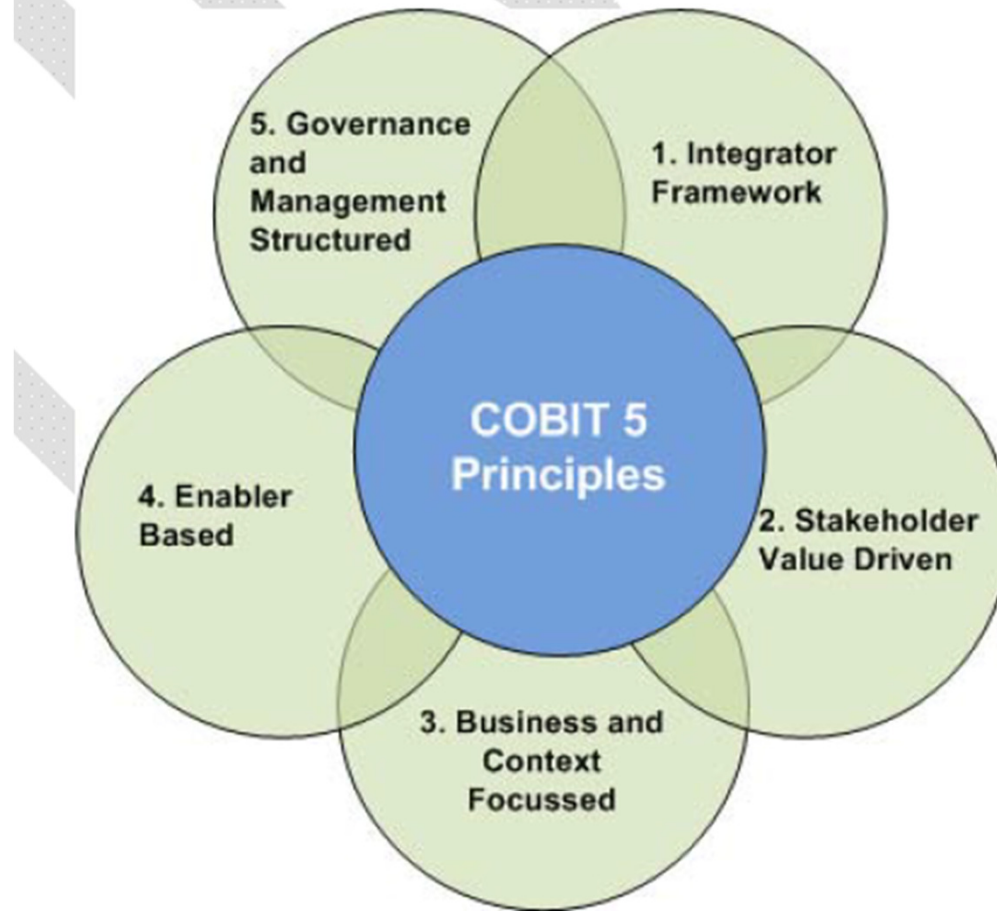
Con COBIT 5

- Se persigue desarrollar un modelo único e integrado de principios, modelos de gobierno, gestión y aseguramiento de TI para sustentar las necesidades de los distintos stakeholders internos y externos de una organización.
 - Para lograrlo COBIT 5 estará organizado en 5 vistas principales, cada una de las cuales incluye los siguientes componentes:
-

Vista	Foco	Componentes principales
Objetivos	¿Por qué los actores hacen lo que hacen?	Riesgos Valor Recursos
Recursos	¿Cómo los actores logran los resultados esperados?	Procesos Información Aplicaciones Personal
Funciones	¿Qué criterios aplican los actores?	Seguridad Privacidad Conformidad
Organizacional	¿Cómo se relacionan los actores en la organización?	TI Proyectos Gestión de servicio
Responsabilidad	¿Quiénes son responsables, ejecutores y aseguran la ejecución?	Gobierno Gestión Aseguramiento

Principios COBIT

Figure 1—COBIT 5 Principles



1. Framework Integrador

- Tiene en cuenta otros estándares como:
 - ❑ COBIT 4.1, Val IT 2, Risk IT, BMIS, etc
 - ❑ ITIL, TOGAF, ISO
-

1. Framework Integrador

- Las pautas para la contribución de TI a la generación de valor para el Negocio, del modelo Val IT 2.0.
 - La existente propuesta de alineamiento Negocio TI, del modelo COBIT 4.1 y 4.2.
 - El enfoque para la mitigación del riesgo corporativo vinculado a TI, del modelo Risk IT.
-

1. Framework Integrador

- La guía de referencia de directrices y buenas prácticas de Auditoría de Sistemas de Información, dadas por el ITAF (IT Assurance Framework).
- Los conceptos básicos y recomendaciones para la sincronización de los programas de Seguridad de la Información con las estrategias corporativas, brindados, recientemente, por el Modelo de Negocio para la Seguridad de la Información, BMIS (Business Model for Information Security)

2. Enfocado en el negocio

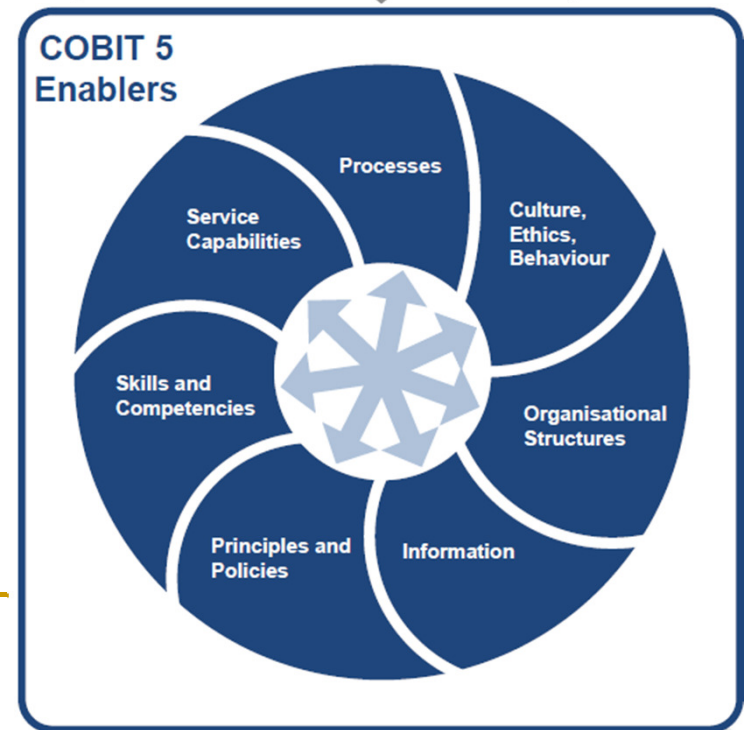
- Las metas y objetivos del negocio son lo más importante
 - De ahí se derivan las metas y objetivos de la organización
-

3. Orientado a proveer valor a los stakeholders

- Objetivo de gobernabilidad:
 - Las empresas comerciales o no existen para crear valor a sus stakeholders
 - Crear valor significa:
 - Lograr beneficios a costos óptimos ajustando (minimizando) los riesgos
 - Como las empresas tienen distintos stakeholders crear valor para ellos puede significar cosas distintas y algunas veces en conflicto entre si.
 - Gobernabilidad es negociar y decidir entre los distintos intereses de valor
 - El sistema de gobernabilidad tiene que considerar en el proceso de toma de decisiones, todos los stakeholders

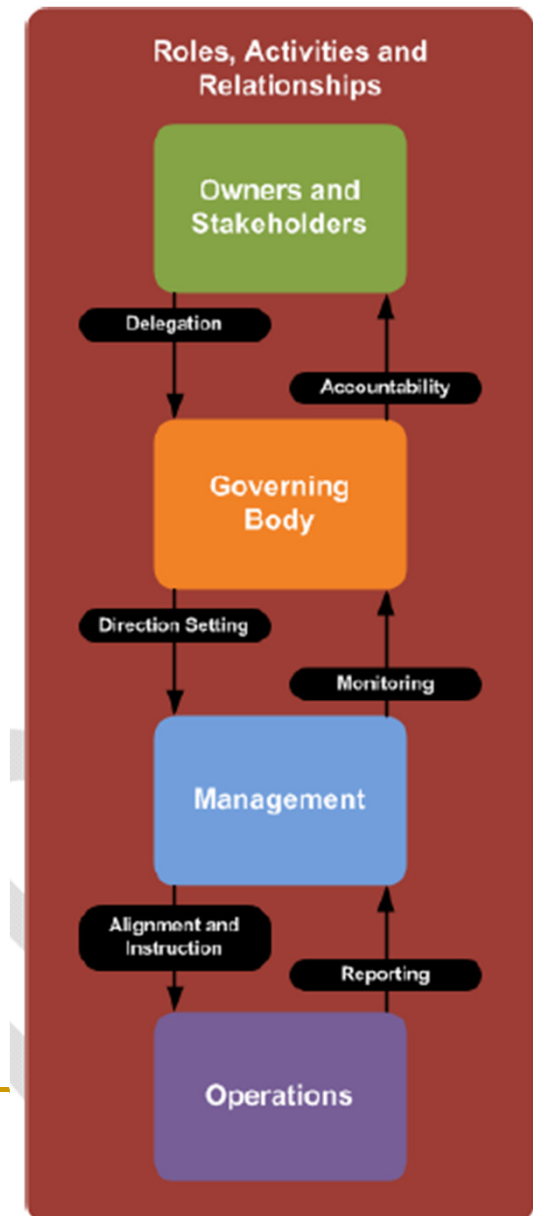
4. Enablers based (Facilitadores, Empoderadores)

- Recursos organizacionales para la gobernabilidad:
 - frameworks, principios, estructura, procesos y prácticas, recursos, servicios capacidades de IT, gente, información.



5. Gobernabilidad y Administración

- Diferencia entre comprometido (gobernabilidad) e involucrado (administración)



Metas de TI

- FINANCIERAS
 - CLIENTE
 - INTERNA
 - APRENDIZAJE Y CRECIMIENTO
-

Metas de TI: Dimensión Financiera

1. Alineamiento de las TI y la estrategia de negocios
 2. Cumplimiento de regulaciones en TI y apoyo para el cumplimiento de leyes y reglamentos externos
 3. Compromiso de la dirección ejecutiva para la toma de las decisiones relacionadas con TI
 4. Administración de riesgos de negocio relacionados con TI
 5. Beneficios logrados desde TI, inversiones y portafolio de servicios
 6. Transparencia de costos, beneficios y riesgos
-

Metas de TI: Dimensión Clientes

- 7. Entrega de servicios de TI en línea con los requisitos de negocio
 - 8. Uso adecuado de las soluciones de aplicaciones, información y tecnología
-

Metas de TI: Dimensión Interna

- 9. Agilidad de entregas de TI
 - 10. Seguridad de la información, el procesamiento y las aplicaciones
 - 11. Optimización de activos de TI, recursos y capacidades
 - 12. Apoyo a los procesos de negocio integrando aplicaciones y tecnología
 - 13. Entrega de los programas a tiempo, en el presupuesto, cumpliendo los requerimientos y las normas de calidad
 - 14. Disponibilidad de la información confiable y útil
 - 15. El cumplimiento de TI con las políticas internas
-

Metas de TI: Dimensión Aprendizaje y crecimiento

- 16. Personal de TI Competente y motivado
 - 17. Conocimientos, experiencia e iniciativas para la innovación del negocio
-

COBIT: Orientación a Procesos

- El marco de trabajo de COBIT proporciona un **modelo de procesos de referencia y un lenguaje común** para que todos en la empresa visualicen y administren las actividades de TI.
 - La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno.
 - También brinda un **marco de trabajo para la medición y monitoreo del desempeño de TI**, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración.
 - Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se **definan las responsabilidades**.
-

Figure 8—COBIT 5 Governance and Management Processes

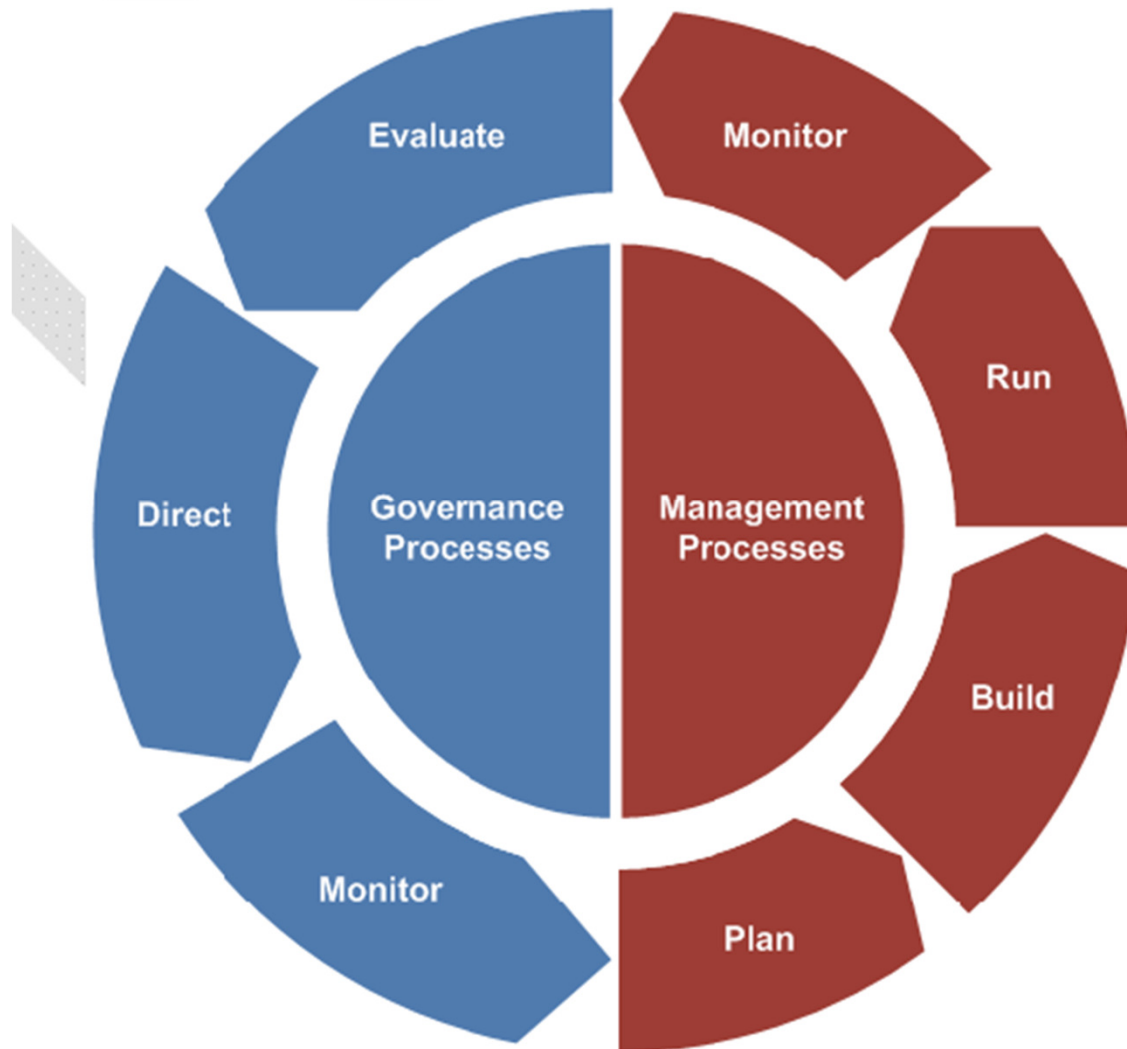
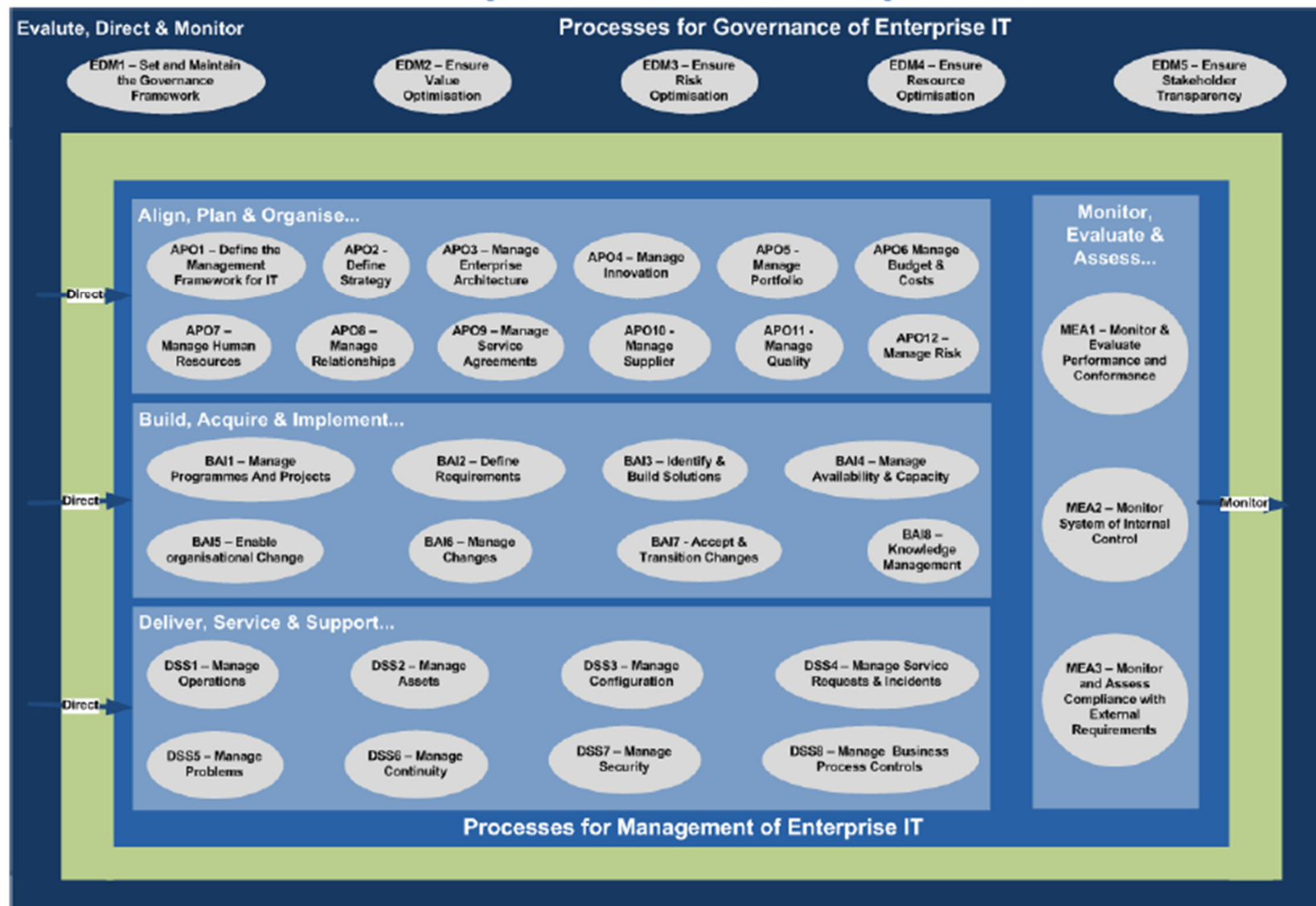


Figure 9—COBIT 5 Illustrative Governance and Management Processes



Evaluar, dirigir y monitorear

- EDM1 Establecer y mantener el marco/modelo de Gobierno
 - EDM2 Asegurar la optimización de valor
 - EDM3 Asegurar la optimización de riesgos
 - EDM4 Asegurar la Optimización de recursos
 - EDM5 Garantizar la transparencia (Integridad/Trazabilidad) a las partes interesadas
-

Alinear, planear y organizar

- APO1 Definir el marco de referencia de la gestión de TI
- APO2 Definir la estrategia (PETI)
- APO3 Gestión de Arquitectura Empresarial
- APO4 Gestionar la innovación
- APO5 Gestionar portafolio de proyectos (PMO)
- APO6 La gestión del presupuesto y los costos
- APO7 Gestión de Recursos Humanos
- APO8 Manejo de las relaciones
- APO9 Gestionar los acuerdos de servicio
- APO10 Gestión de Proveedores y Contratistas
- APO11 Gestión de Calidad
- APO12 Gestionar el riesgo

Construir, adquirir, implementar

- BAI1 Gestión Programas y Proyectos
 - BAI2 Definir los requerimientos
 - BAI3 Identificar y construir soluciones
 - BAI4 Administrar la disponibilidad y capacidad
 - BAI5 Habilitar Cambio Organizacional
 - BAI6 Gestionar los cambios
 - BAI7 Aceptar y la transición del cambio
 - BAI8 Gestión del Conocimiento
-

Entrega, servicio y soporte

- DSS1 Gestión de operaciones
 - DSS2 Gestionar los activos
 - Dss3 Gestionar configuración (CMDB)
 - DSS4 Gestionar las solicitudes de servicio (Mesa de servicios) e incidentes
 - DSS5 Manejar los problemas (Soluciones de raíz)
 - DSS6 Gestión de la continuidad
 - DSS7 Administrar la seguridad Informática
 - DSS8 Gestionar los controles en los procesos de negocio
-

Monitorear, evaluar y valorar

- MEA1 Monitorear y evaluar el desempeño y el cumplimiento (la conformidad)
 - MEA2 Monitorear el Sistema de Control Interno
 - MEA3 Monitorear y evaluar el cumplimiento de los requisitos externos
-

El Modelo de Madurez

- Es una forma de medir el grado de desarrollo de los procesos de la organización.
- Este modelo define perfiles de organizaciones, en relación a los progresos en el gobierno de TI.
- Atiende aspectos tales como :
 - el grado de formalidad con que se cumplen los procesos
 - el reconocimiento de que existen problemas
 - las posibilidades de entrenamiento y capacitación
 - el grado de automatización de los procesos
 - el nivel de avance de la organización en materia de administración del conocimiento relativo a buenas prácticas en TI.

El Modelo de Madurez

- 0 Inexistente
 - Hay una absoluta carencia de procesos reconocibles.
 - La organización no ha reconocido que haya una necesidad de acciones en ese sentido.
-

El Modelo de Madurez (cont.)

■ 1 Inicial/Ad Hoc

- ❑ Hay evidencia de que la organización ha reconocido que existen problemas y necesitan ser tratados.
 - ❑ No hay procesos estandarizados sino que por el contrario hay acercamientos puntuales que tienden a ser aplicados solo por un individuo o a un caso concreto.
 - ❑ La aproximación global de la gerencia al tema no es planificada ni proactiva.
-

El Modelo de Madurez (cont.)

- 2 Repetitivo pero intuitivo
 - ❑ Los procesos se encuentran en una etapa en la cual diversos grupos que emprenden la misma tarea siguen procedimientos similares.
 - ❑ No hay ningún entrenamiento formal o comunicación estándar de procedimientos
 - ❑ La responsabilidad descansa en los individuos.
 - ❑ Hay un alto grado de confianza en el conocimiento de los individuos y por lo tanto los errores son probables.
-

El Modelo de Madurez (cont.)

■ 3 Definido

- ❑ Los procedimientos están estandarizados y se han documentado.
 - ❑ Se han comunicado mediante el entrenamiento.
 - ❑ Los individuos deciden seguir o no estos procesos.
 - ❑ Es difícil que las desviaciones sean detectadas.
 - ❑ Los procedimientos en si mismos, no son sofisticados sino que son la formalización de practicas existentes.
-

El Modelo de Madurez (cont.)

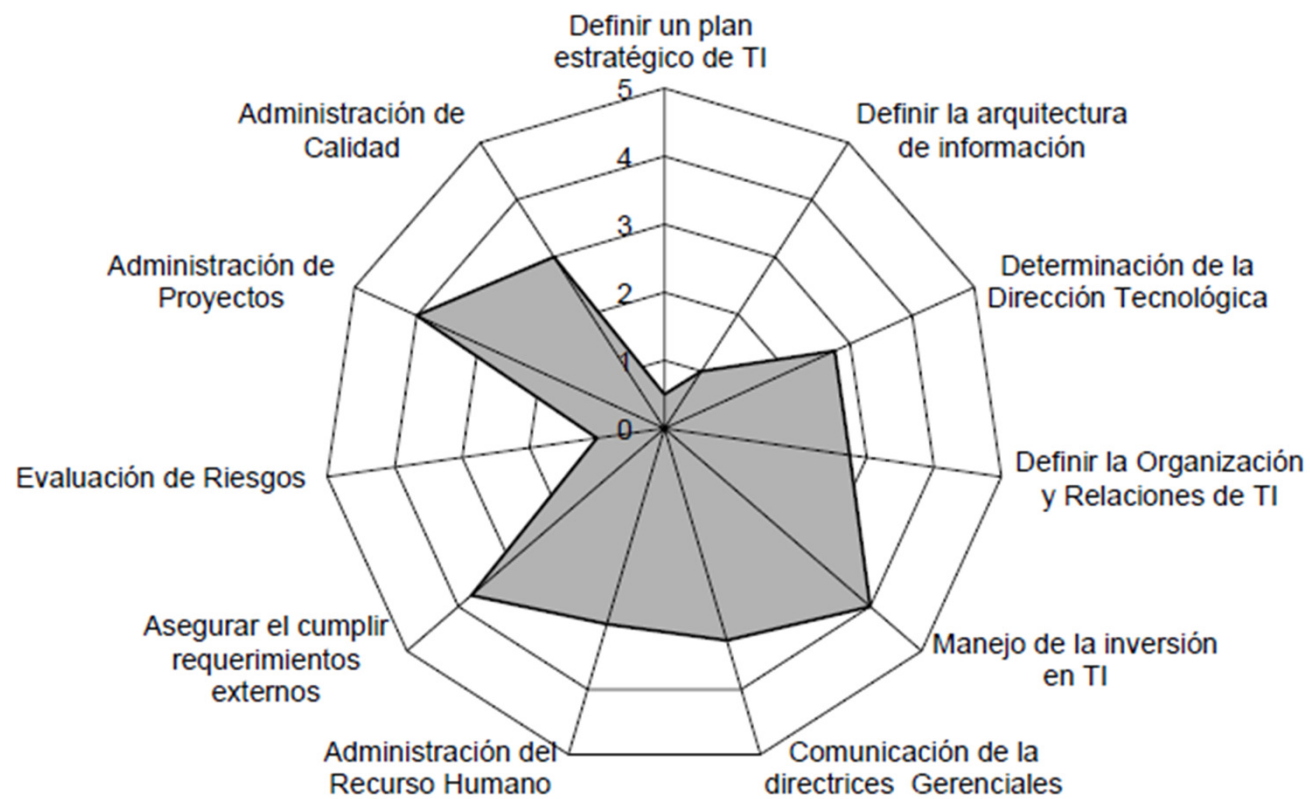
■ 4 Administrado y Medible

- ❑ Es posible vigilar y medir el cumplimiento de los procedimientos y tomar acciones en los casos en los que los procesos resultan no trabajar con eficacia.
 - ❑ Los procesos están bajo mejora constante y proporcionan buenas practicas aplicables.
 - ❑ La automatización y las herramientas se utilizan en una manera limitada o de modo parcial.
-

El Modelo de Madurez (cont.)

■ 5 Optimizado

- ❑ Los procesos de TI se han refinado al nivel de la mejor practica, basándose los resultados en la mejora continua y las iniciativas en materia de madurez que toma como modelo a otras organizaciones.
 - ❑ La tecnología se utiliza como un camino integrado para automatizar el proceso de trabajo, proporcionando calidad y eficacia a las herramientas para mejorar, haciendo que la empresa se adapte rápidamente a los cambios.
-



Descripción del Proceso

Establecer un marco común que consiste en procesos de negocio, información, datos, aplicaciones y las capas de la arquitectura tecnológica para la realización eficaz y eficiente de las estrategias de la empresa y de TI, mediante la creación de modelos y prácticas claves que describan la arquitectura actual (línea de base, as-is) y las arquitecturas de destino (to-be).

Definir los requerimientos para la taxonomía, normas, directrices, procedimientos, modelos y herramientas, y proporcionar un vínculo para estos componentes.

Mejorar la alineación, aumentar la agilidad, mejorar la calidad de la información y generar un ahorro potencial de costos a través de iniciativas tales como la reutilización de activos.

APO03 Manage Enterprise Architecture

Area: Management

Domain: Align, Plan and Organise

Propósito del Proceso

Representar los diversos componentes que conforman la empresa y sus relaciones inter -, así como los principios rectores de su diseño y evolución en el tiempo, que permita una entrega estándar, a tiempo y eficiente de los objetivos operativos y estratégicos.

APO03 Manage Enterprise Architecture	Area: Management Domain: Align, Plan and Organise
--------------------------------------	--

Prácticas

APO03.01 Desarrollar la visión de la arquitectura empresarial

APO03.02 Definir la arquitectura de referencia

APO03.03 Seleccionar oportunidades y decisiones

APO03.04 Definir la implementación de la arquitectura

AP003.05 Proveer los servicios de la arquitectura empresarial

Descripción del Proceso

Identificar soluciones y analizar los requerimientos antes de la adquisición o creación de soluciones de TI, para asegurarse de que están en línea con los requisitos de la empresa, que cubre los procesos de negocio, aplicaciones, información / datos, infraestructura y servicios.

Revisar las opciones factibles incluyendo los costos y beneficios relativos, análisis de riesgos, y la aprobación de los requisitos y las soluciones propuestas.

BAI02 Define Requirements

Area: Management

Domain: Build, Acquire and Implement

Propósito del Proceso

Crear óptimas soluciones factible que satisfagan las necesidades de la empresa, minimizando los riesgos.

BAI02 Define Requirements

Area: Management

Domain: Build, Acquire and Implement

Prácticas

BAI02.01 Definir y mantener los requerimientos técnicos y funcionales del negocio

BAI02.02 Realizar estudios de factibilidad y formular alternativas de solución

BAI02.03 Gestionar los riesgos de los requerimientos

BAI02.04 Obtener la aprobación de los requerimientos y de las soluciones
