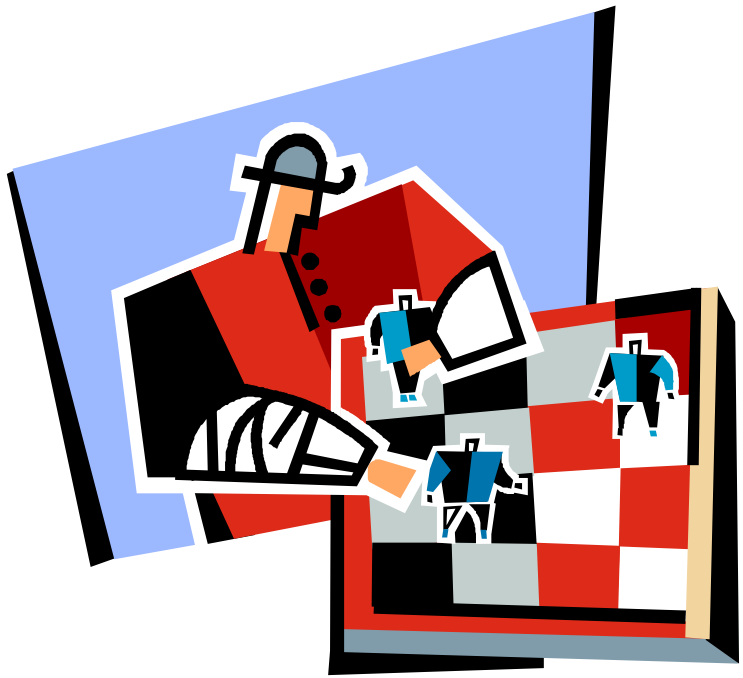
Riesgo Empresarial:
Identificación, Gobierno y Administración del Riesgo de TI

El Marco de Riesgo de TI

Edmundo Treviño Gelover,
CGEIT, CISM, CISA

Definiciones en Evolución

- Los conceptos tradicionales de riesgo, auditoría y control han evolucionado hacia conceptos mas amplios como el Corporate Governance y el IT Governance; producto de las estrictas regulaciones sobre el control interno, el riesgo operacional, las responsabilidades de la alta Gerencia y la necesidad de alinear la TI con la estrategia del negocio.



El IT Governance

El Gobierno Corporativo refiere a cómo una organización, a través de varios roles y responsabilidades de sus Directores y de la propia Administración:

- Fija los objetivos corporativos
- Ejecuta las operaciones diarias del negocio
- Monitorea el desempeño de la organización y su personal
- Integra a sus stakeholders
- Alinea el comportamiento y las actividades corporativas
- Cumple con leyes y regulaciones aplicables

El IT Governance:

Parte integral del Gobierno Corporativo.

Contempla el liderazgo, estructuras de organización y procesos que aseguran que la Tecnología de la Información, soporta los objetivos y estrategias de la organización

IT Governance Institute *

Expectativas sobre la TI

- **¿ Logrará la TI sus objetivos ?**
- **¿ Podrá la TI adaptarse a los nuevos escenarios ?**
- **¿ Conoce y/o administra la TI sus riesgos ?**
- **¿ Existe una alineación de objetivos y esfuerzos entre TI y la gestión empresarial ?**

La alta Gerencia espera:

- Apoyo de la tecnología para alcanzar los objetivos del negocio, p.ej. en la Banca: uso intensivo de sistemas y medios electrónicos para hacer llegar a los clientes, el portafolio de productos y servicios financieros.
- Manejo razonable de costos e inversión de la TI.
- Incremento en eficiencia y reducción de riesgos.
- Cumplimiento con regulaciones y normatividad.
- Mayor rentabilidad.

Expectativas sobre la TI

- **¿ Logrará la TI sus objetivos ?**
- **¿ Podrá la TI adaptarse a los nuevos escenarios ?**
- **¿ Conoce y/o administra la TI sus riesgos ?**
- **¿ Existe una alineación de objetivos y esfuerzos entre TI y la gestión empresarial ?**

El propio Director de Sistemas busca:

- Asegurar la continuidad operativa de los servicios otorgados a los usuarios y clientes.
- Aprovechar los sistemas aplicativos y su infraestructura, sin perder de vista la evolución de la tecnología.
- Atención a la seguridad y administración del riesgo tecnológico.
- Cumplimiento presupuestal y atención de requerimientos regulatorios.

El Riesgo asociado a la TI

Aún y cuando los conceptos de IT Governance son entendidos y las necesidades y expectativas en el uso de la tecnología resultan claras para todos, es común seguir observando entre otros, los siguientes hechos:

- La IT sigue estando esta expuesta a riesgos relacionados con: la seguridad de sus sistemas, la continuidad del servicio, los fraudes, daños en la infraestructura, perdidas o alteraciones de información sensible, multas o penalizaciones, incidentes operativos, daños físicos y ambientales, etc.
- Los sistemas aplicativos y su infraestructura, no cubren las expectativas para el negocio o simplemente son desaprovechados.
- Ausencia de Gobierno de TI: Las prácticas de operación y control de la TI son informales, existen muchos re-trabajos, tiempos elevados para realizar mantenimientos de aplicaciones, cuellos de botella en proyectos, niveles bajos de calidad en el servicio, deficiente organización de las actividades internas.
- El área encargada de IT es vista como un área de “gasto permanente” y no se muestra aún ningún retorno a la inversión.

Necesidad de un Marco de Riesgo

- Con base en lo anterior, surge la necesidad de crear un Marco de referencia que permita:
  - Reconocer la existencia de riesgos de TI,
  - Facilite su identificación, evaluación y administración,
  - Que reconozca que existe una dependencia muy importante del negocio, hacia el funcionamiento continuo de la TI
  - Y por ende ..hacia el manejo de sus riesgos….!!

Antecedentes

- El IT Governance Institute expuso recientemente un draft de la publicación próxima a liberar denominada **Enterprise Risk: Identify, Govern and Manage Risk, The Risk IT Framework.**

- El Marco de Riesgos de TI (The Risk IT Framework) es producto de la investigación y aporte de la experiencia conjunta de un equipo global de especialistas, cuya misión fue la de facilitar a la alta Gerencia, una administración efectiva de los riesgos de TI relacionados con el negocio, a partir de su identificación y evaluación.

- Este marco representa el eslabón perdido entre el ERM (Enterprise Risk Management) y el IT Risk Management, cubriendo además en su totalidad el Marco IT Governance del ITGI. Asimismo, este marco se constituyó a partir de los componentes de riesgo relacionados dentro de los marcos actuales, es decir: COBIT y Val IT.

Antecedentes

- El riesgo de TI es el riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI dentro de la empresa. Este riesgo consiste en los eventos relacionados con la TI que pueden potencialmente impactar al negocio. Cada evento puede ser visto como **Riesgo y Oportunidad**

La TI como Inhibidor de Valor o Destructor

El Riesgo de TI

- Eventos adversos relacionados con TI que destruyen valor
- Valor de negocio no realizado o reducido a través de la TI
- Oportunidades omitidas de asistencia de TI

Oportunidad de TI

- Identificación de nuevas oportunidades de negocio a través del uso de la TI
- Incremento del valor del negocio a través del uso óptimo de las capacidades de TI

La TI como Habilitador de Valor

Marco de Riesgo de TI

Principios y Bases

- El Marco de Riesgo de TI que plantea el ITGI, explica los riesgos de TI y ayuda a quienes lo aplican para:
  - Integrar la administración de los riesgos de TI, dentro de la administración general de los riesgos empresariales y estructuras de cumplimiento.
  - Tomar decisiones bien informadas acerca del alcance del riesgo, del apetito al riesgo y su nivel de tolerancia.
  - Entender cómo responder al riesgo.

Marco de Riesgo de TI

Principios y Bases

- Además, este Marco de Riesgo de TI atiende muchos aspectos que las organizaciones enfrentan actualmente y provee:
  - Una apreciación muy atinada de los riesgos relacionados de TI presentes y de futuro inmediato, a través de toda la organización y de las bases con las cuales la organización puede atenderlos.
  - Una guía punta-a-punta de cómo administrar los riesgos relacionados de TI, mas allá del alcance puramente técnico y de sus medidas de control y seguridad.
  - Un entendimiento de cómo capitalizar la inversión hecha en un sistema de control interno de TI ya establecido, para administrar los riesgos relacionados de TI.

Marco de Riesgo de TI

Principios y Bases

- Un marco/lenguaje común para ayudar a administrar la relación entre los tomadores de decisiones (Comités / Alta Dirección), el CIO y la Gerencia a cargo de la administración de riesgos empresariales, ó entre los Auditores y la propia Dirección.

- La promoción y la responsabilidad de los riesgos y su aceptación a través de toda la organización.

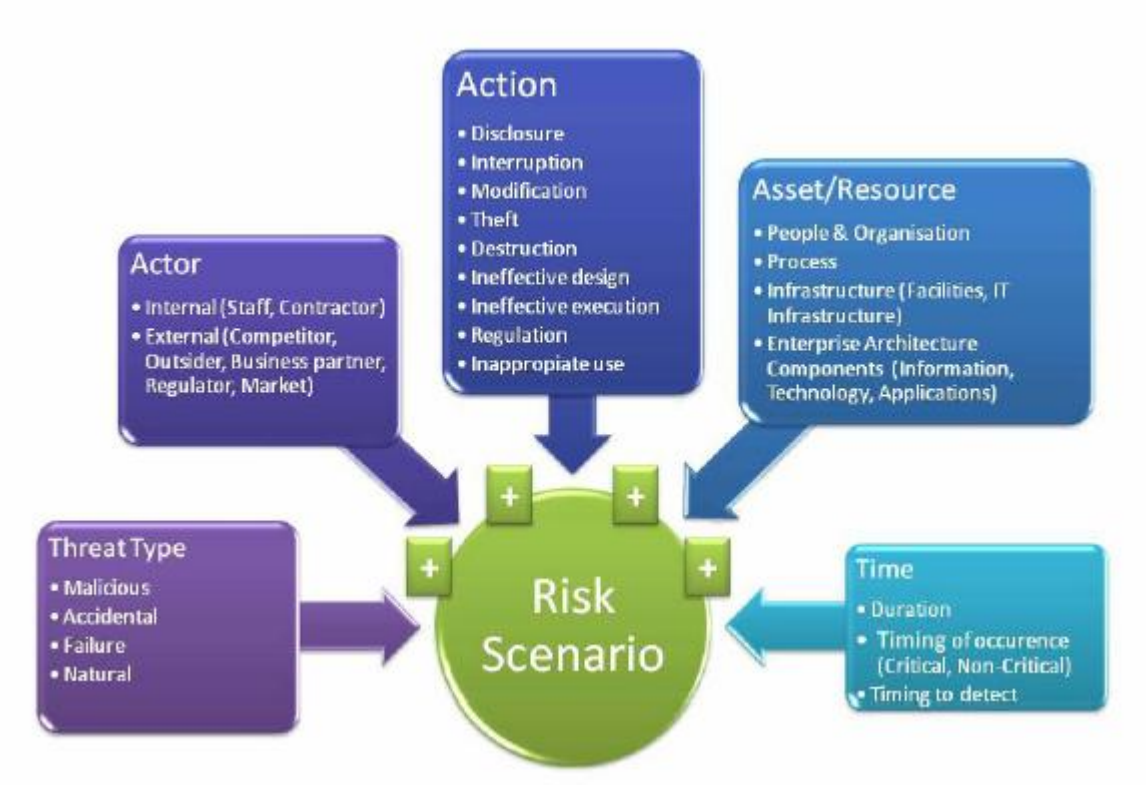
Marco de Riesgo de TI

¿ A quienes esta dirigido?

- A la alta Dirección y a sus Comités, quienes necesitan fijar el direccionamiento y monitoreo de los riesgos de toda la organización.
- Gerentes de TI y departamentos de negocio, quienes necesitan definir un proceso de administración de riesgos.
- Responsables y profesionales de administración de riesgos, quienes necesitan guías específicas para el manejo del riesgo de TI.
- Externos relacionados.

Fundamento del Riesgo de TI

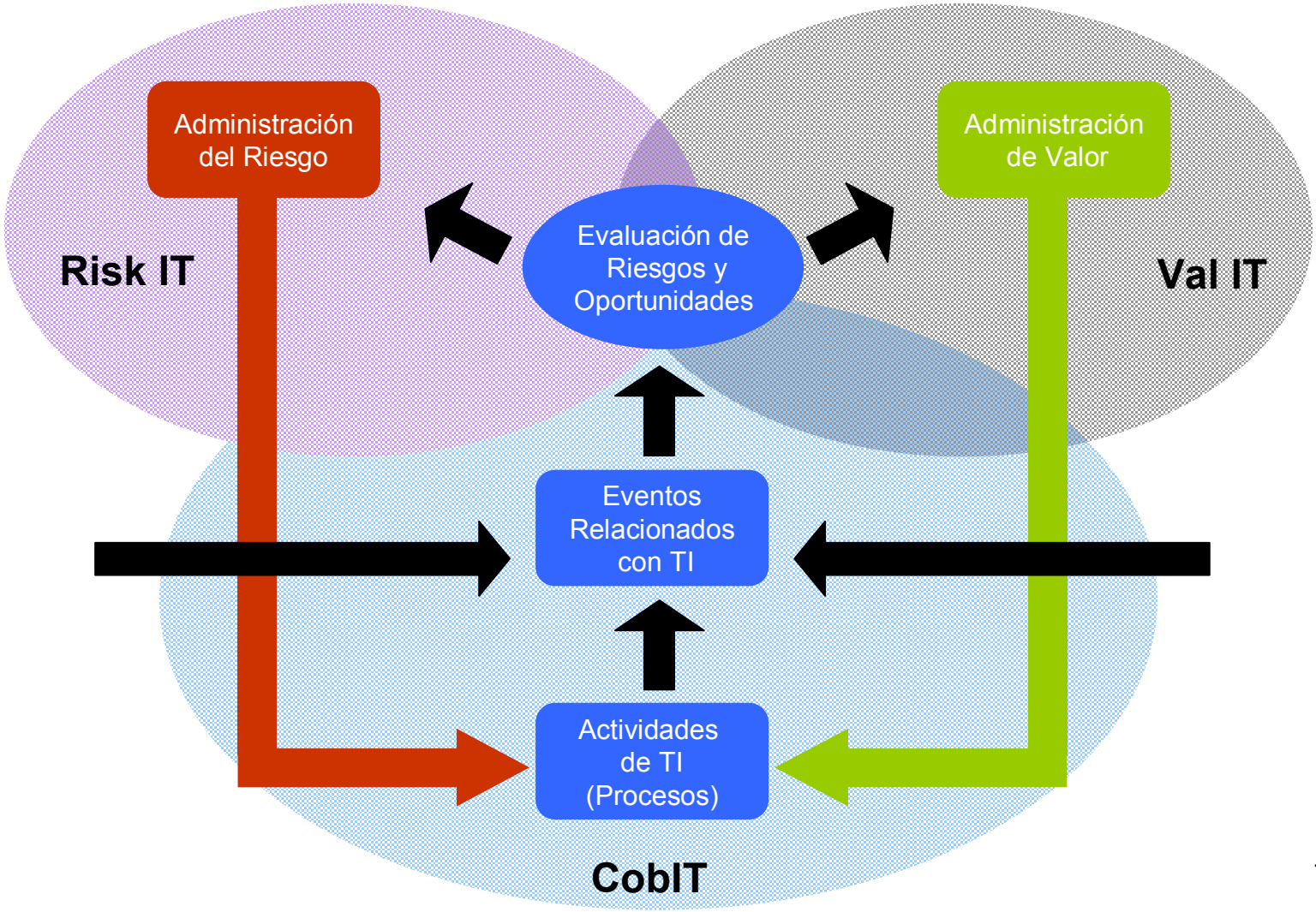
Escenarios de Riesgo



Un primer paso es identificar, entender y evaluar el riesgo de TI considerando todo lo que puede salir mal con o en relación a TI; usando para ello escenarios de riesgo, los cuales contienen varios componentes.

Los 3 Marcos del ITGI

Riesgos, oportunidades y su tratamiento

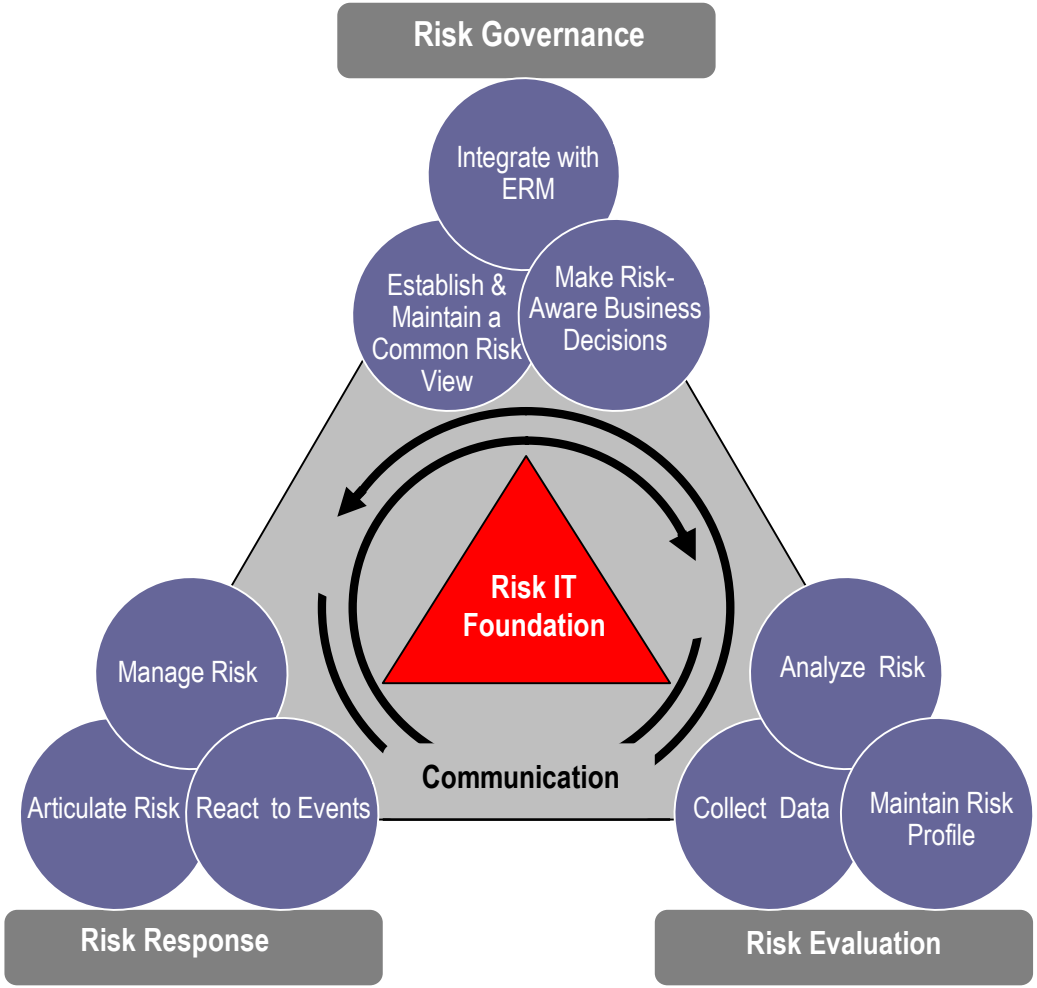


Componentes de Riesgo de TI

El Marco tiene tres dominios: **Risk Governance, Risk Evaluation** y **Risk Response** divididos en 9 procesos de negocio. Cada uno contiene los siguientes 3 procesos:

- Risk Governance (Gobierno del Riesgo)
  - Establecimiento y Mantenimiento de una Visión Común de Riesgo
  - Integración con ERM (Enterprise Risk Management)
  - Toma de Decisiones de Negocio con una Conciencia del Riesgo
- Risk Evaluation (Evaluación del Riesgo)
  - Recolección de Datos
  - Análisis de Riesgo
  - Mantenimiento del Perfil de Riesgos
- Risk Response (Respuesta al Riesgo)
  - Articulando el Riesgo
  - Administrando el Riesgo
  - Reaccionando a Eventos

Componentes de Riesgo de TI



Administrando el riesgo en la práctica

Guía Técnica

Existen guías técnicas que complementan el Marco de Riesgo de TI y que proveen ejemplos de posibles técnicas a emplear para su tratamiento, algunas de ellas incluyen:

- Construcción de escenarios a partir de escenarios genéricos de riesgo de TI.
- Construcción de un mapa de riesgos, usando técnicas para describir el impacto y frecuencia de los escenarios.
- Construcción de criterios de impacto con relevancia al negocio.
- Uso de COBiT y Val IT para mitigar los riesgos, la liga entre el riesgo y los objetivos de control de COBiT y Val IT, y prácticas clave de administración.

Administrando el riesgo en la práctica

Guía Técnica

—Techniques Guide Overview									
Domain/Process	Risk Governance			Risk Evaluation			Risk Response		
Technique/Guidance	RG1 Establish and Maintain a Common Risk View	RG2 Integrate with Enterprise Risk Management	RG3 Make Risk-aware Business Decisions	RE1 Collect Data	RE2 Analyse Risk	RE3 Maintain Risk Profile	RR1 Articulate Risk	RR2 Manage Risk	RR3 React to Events
1 Defining a risk universe and scoping	■	■	■						
2 Constructing risk scenarios				■	■	■	■		
3 Sample generic IT risk scenarios				■	■	■	■		
4 Describing risk—expressing impact in business terms	■	■			■		■		
5 Describing risk—COBIT business goals mapping with other impact criteria	■	■			■		■		
6 Describing risk—qualitative and quantitative methods	■	■			■		■	■	
7 Describing risk—expressing impact	■	■			■		■	■	
8 Describing risk—expressing frequency	■	■			■		■	■	
9 Risk factors in the risk assessment process	■	■	■		■		■	■	
10 Describing risk—risk maps, risk register?	■	■	■		■	■	■		
11 Defining risk appetite and risk tolerance	■	■	■		■	■	■		
12 A risk analysis workflow					■				
13 Risk aggregation					■	■	■	■	
14 Key risk indicators and risk reporting	■	■	■	■			■	■	
15 Risk response and prioritisation				■				■	■
16 Using COBIT and Val IT to map controls to risk scenarios				■				■	■
17 Risk profiles	■	■				■	■		
18 Risk communication flows	■	■	■	■	■	■	■	■	■
Appendix I—How COBIT and Val IT practices can help manage risk								■	■
Appendix II—Risk management principles and practices in Risk IT vs. other frameworks	■	■	■	■	■	■	■	■	■

Componentes de Riesgo de TI

El Marco también provee:

- Guías Gerenciales (Management Guidelines) que pueden ser usadas para confeccionar los procesos al ambiente de cada organización.
- Estas Guías Gerenciales incluyen Objetivos, Métricas (a diferentes niveles) y Matrices RACI (Responsible, Accountable, Consulted and Informed).
- Para facilitar las comparaciones y benchmarks también existe un modelo de madurez para cada dominio, el cual emplea una escala incremental de 0 a 5.

Componentes de Riesgo de TI

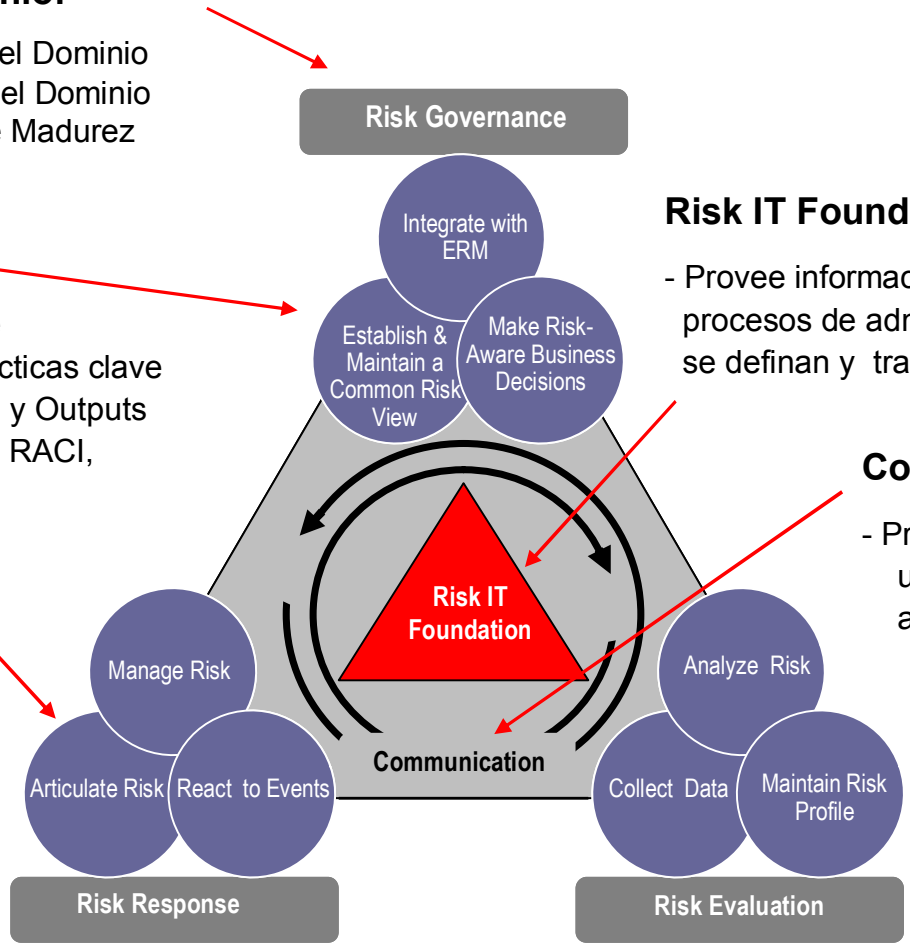
Nivel de Información

Por Dominio:

- Objetivo del Dominio
- Métricas del Dominio
- Modelo de Madurez

Por Proceso:

- Objetivo y Actividades Clave
- Los procesos en detalle: prácticas clave de administración con Inputs y Outputs
- Guías Gerenciales: Matrices RACI, Objetivos y Métricas



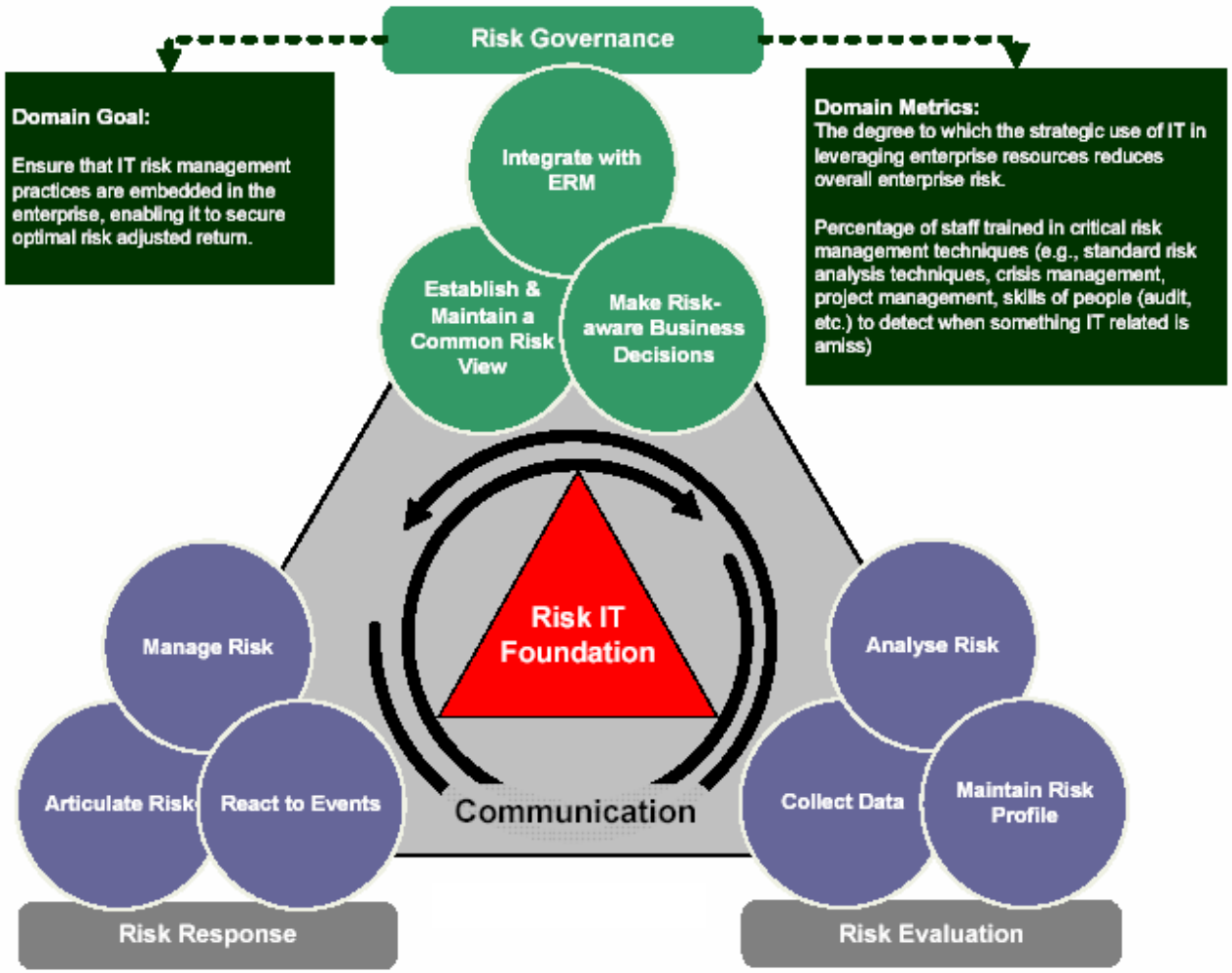
Risk IT Foundation:

- Provee información para que los procesos de administración de riesgo se definan y trabajen.

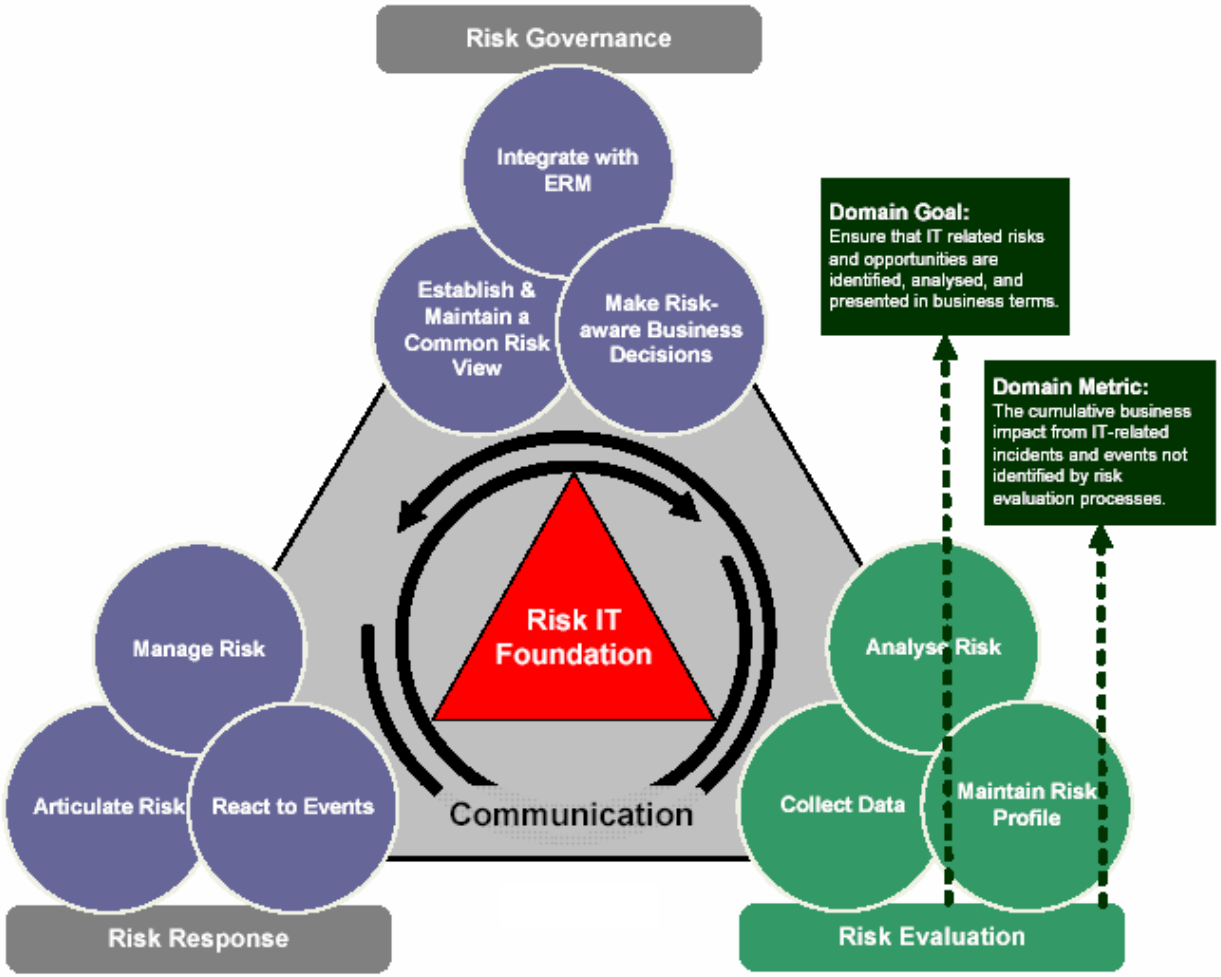
Comunicación:

- Propone un flujo para crear una comunicación efectiva a partir del cumplimiento y seguimiento de políticas, competencias y administración de los datos de riesgo.

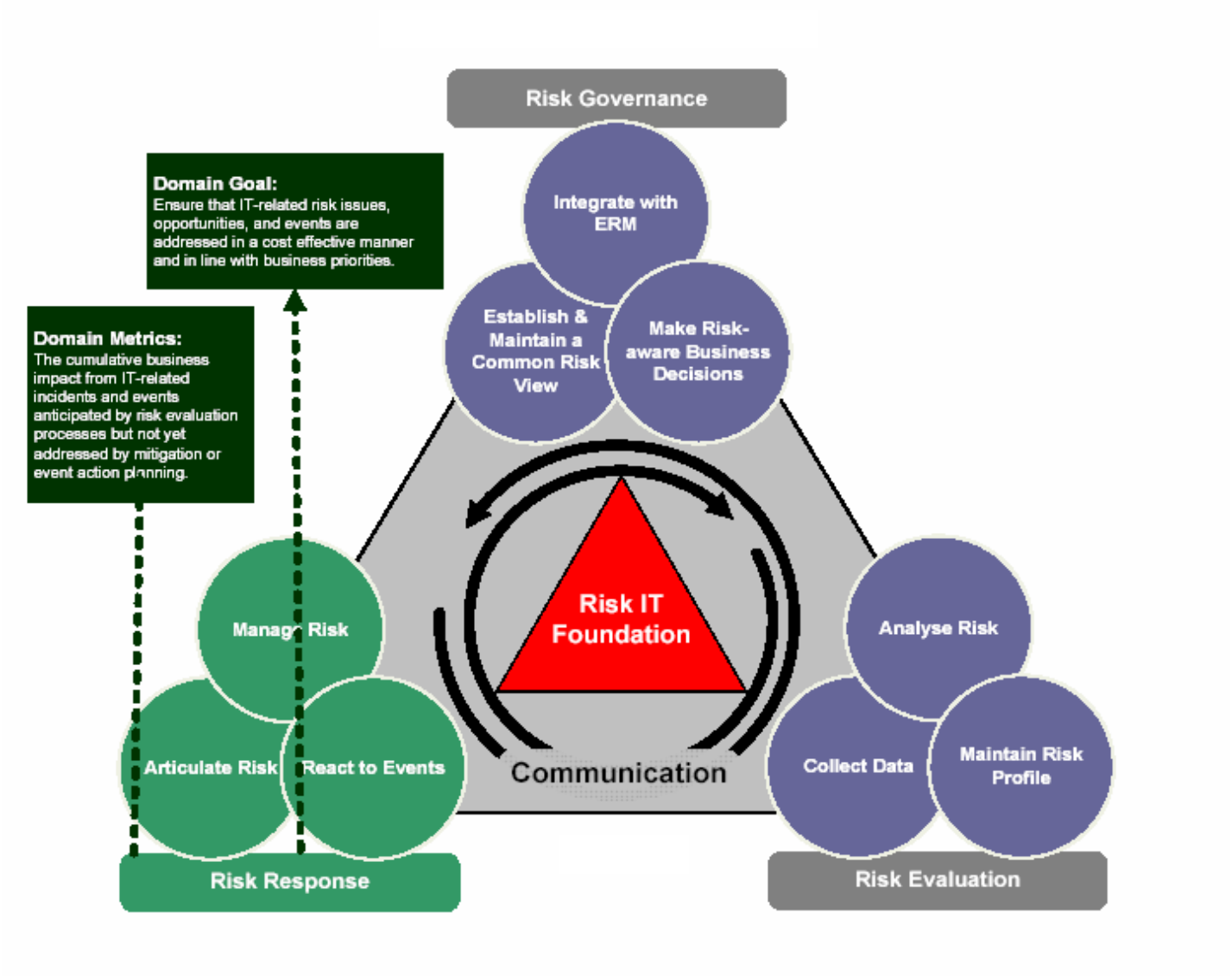
Información por Dominio



Información por Dominio

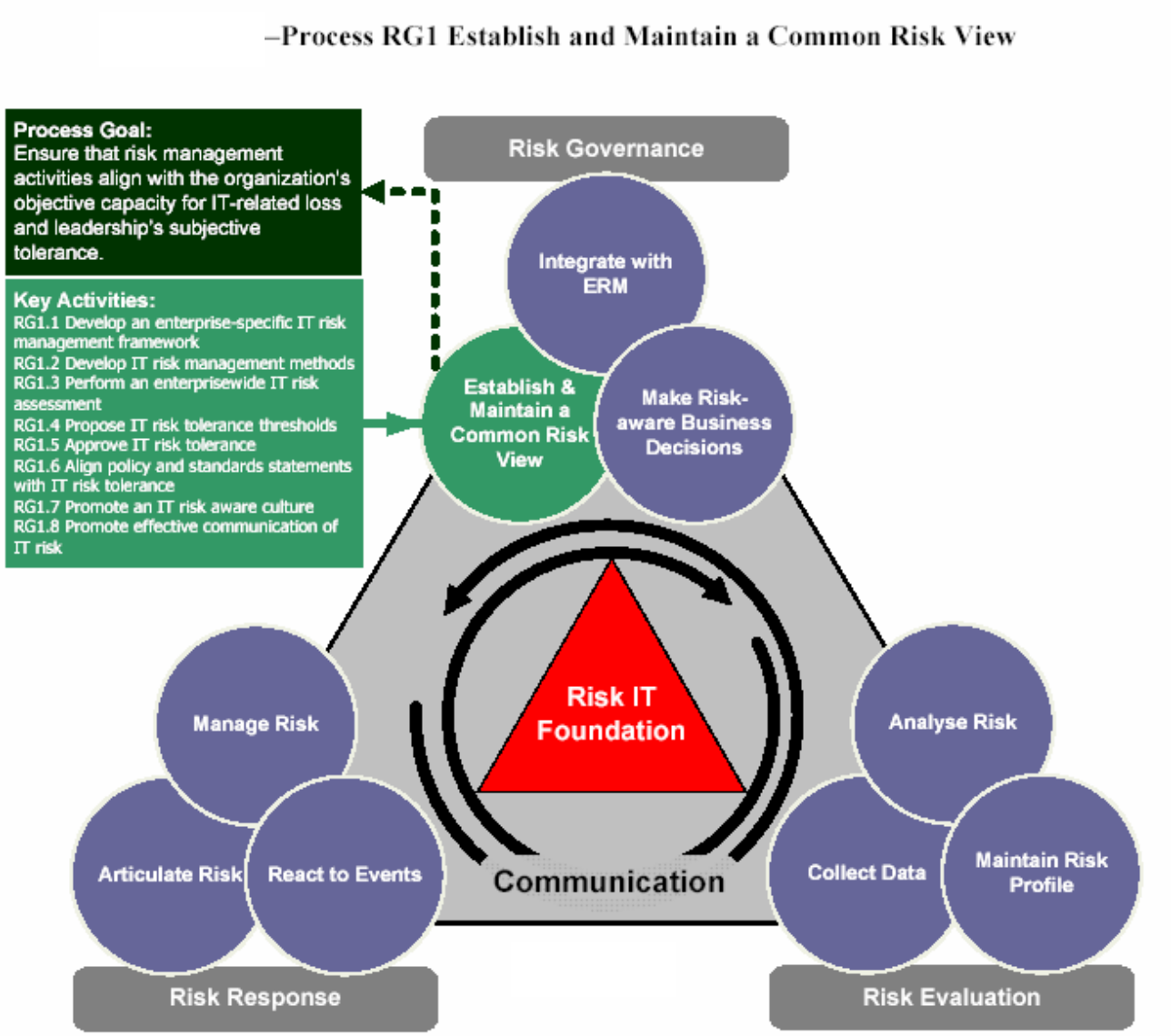


Información por Dominio



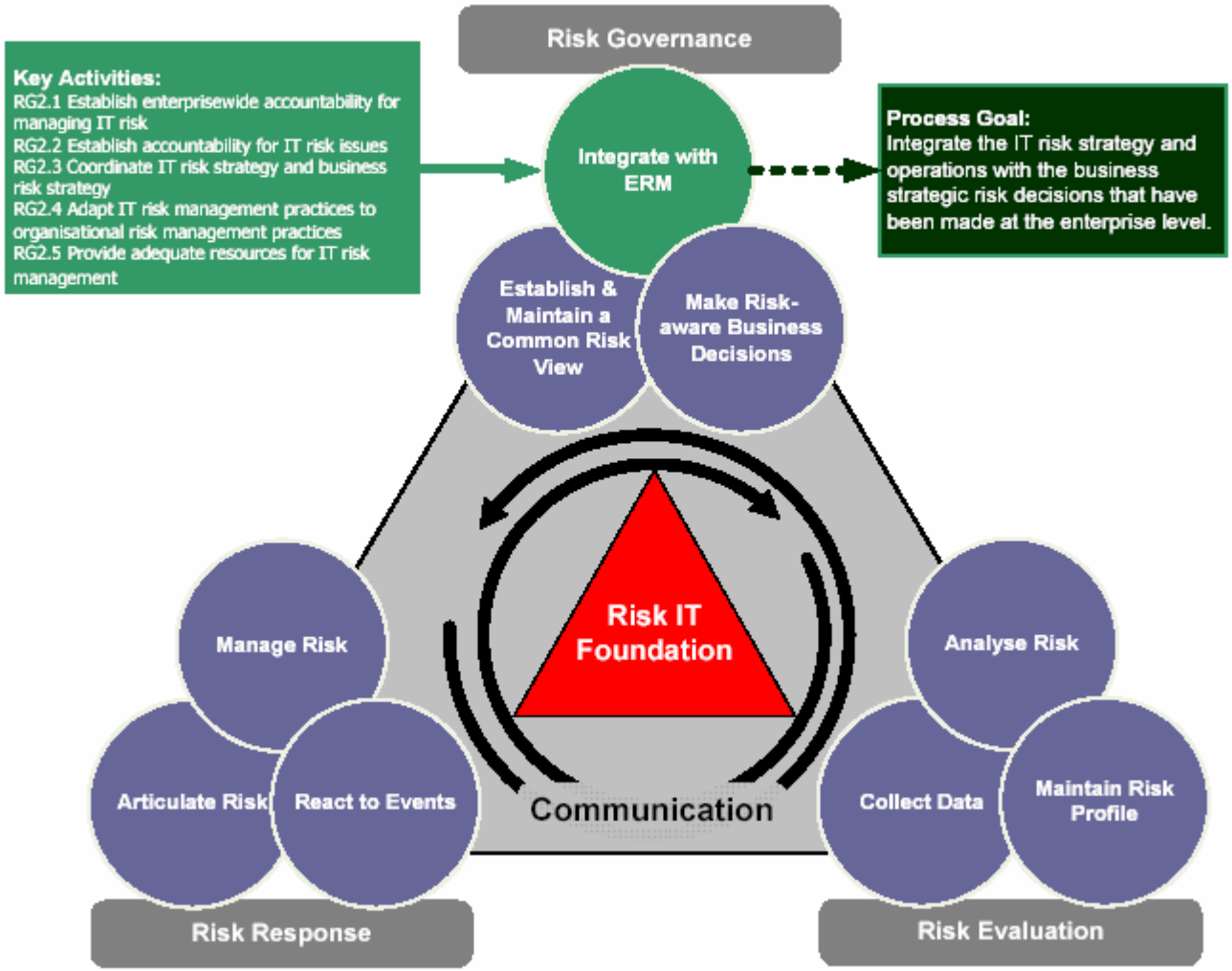
Información por Proceso

–Process RG1 Establish and Maintain a Common Risk View

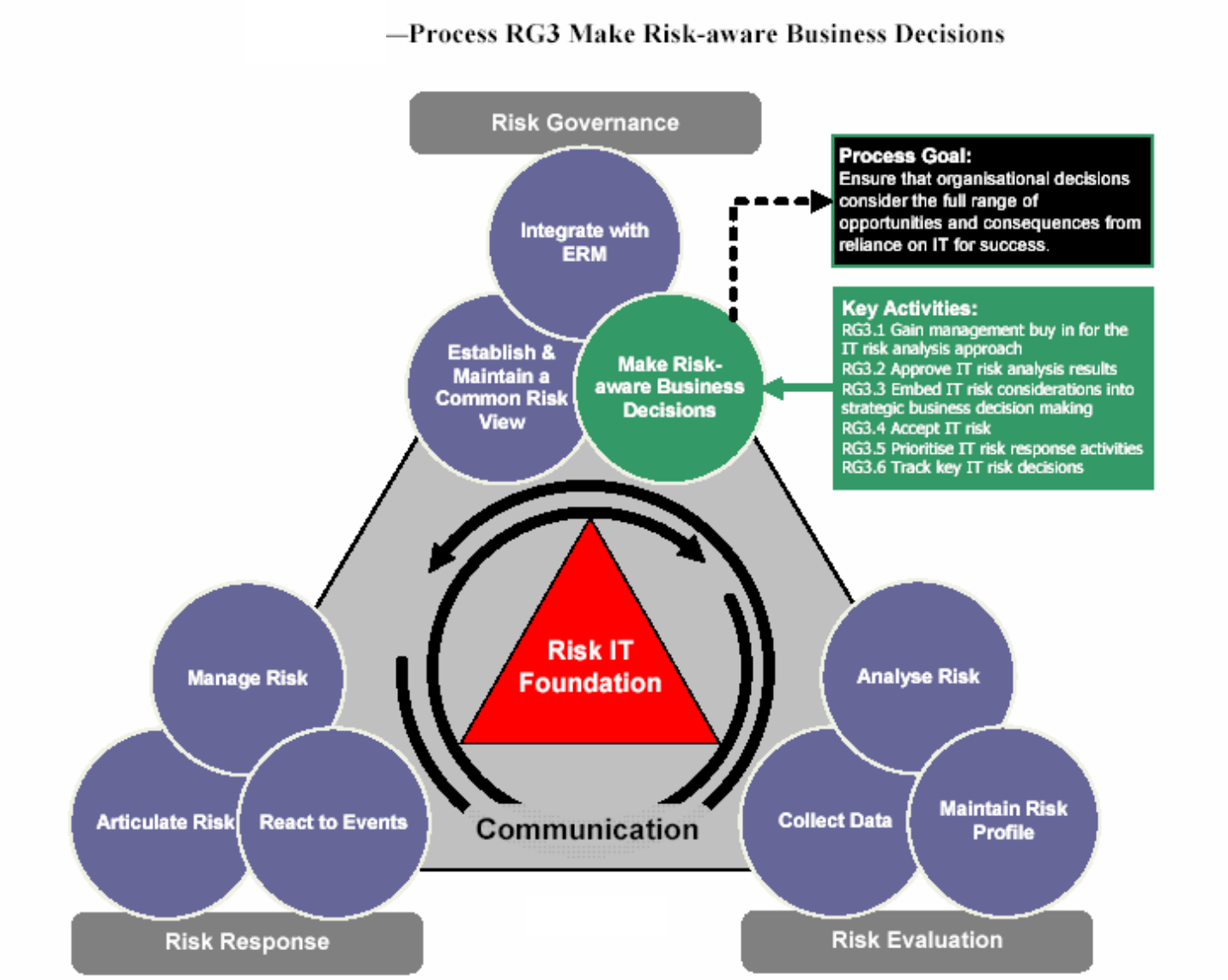


Información por Proceso

—Process RG2 Integrate with ERM



Información por Proceso



Información por Proceso

PROCESS DETAIL

RG1 Establish and Maintain a Common Risk View

RG1.1 Develop an enterprise-specific IT risk management framework.

Determine how IT-related risk management is to be defined in the context of protecting a given business process or business activity. Establish principles and guidelines for data modelling; integration of IT risk into strategic plans; risk identification, measurement, evaluation, and assessment (e.g., maintaining alignment with the entity's objectives, risk appetite, and tolerance); and risk monitoring, reporting, and response. Classify IT risk factors, events and their potential impacts. Define the relationships between those authorised to take certain types of IT risk and those responsible for evaluating and responding to IT risk. Define risk rating scales (e.g., frequency, magnitude); control categories (e.g., predictive, detective, corrective); and hierarchies for risk-based policies, standards, and operating procedures. Where available, embed existing enterprise-wide risk management principles and views of risk (e.g., actuarial view, portfolio view, predictive systems view). Determine when and how certain enterprise risk views are to be used for IT risk. Tailor the framework to accommodate the enterprise's unique performance needs and external requirements.

From	Inputs
RG1.3, COBIT ME4	Enterprise appetite for IT risk
RG2.3	IT risk management scope
RG2.3	Enterprise integrated risk reporting requirements
RG2.4	Updates to IT risk management framework
COBIT PO9	IT-related risk management guidelines
*	Enterprise risk management framework

To	Outputs
RG1.2, RG1.3, RG1.8, RE2.1	IT risk management framework

Información por Proceso

RG1.2 Develop IT risk management methods.
Define requirements for operating within the IT risk management framework. Include methods to 1) understand the business context for IT (e.g., business activity IT dependency analysis, scenario analysis); 2) identify IT risk (e.g., data model, escalation pathways); 3) govern IT risk (e.g., enterprise-wide IT risk assessment procedures, risk-based decision models); and 4) respond to IT risk and minimise the impact of IT-related events. In addition, establish monitoring methods to maintain and improve IT risk management processes (e.g., select the right KRIs for the right business performance targets and define escalation procedures). Work with the board to obtain reasonable assurance that the methods and practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite.

From	Inputs
RG1.1	IT risk management framework
RG2.3	IT risk management scope
RG2.4	Updates to IT risk management methods
RG2.4	Updates to IT risk management process monitoring methods
RR3.4	Process improvements
COBIT PO9	IT-related risk management guidelines
*	Enterprise risk management framework

To	Outputs
RG1.3, RG1.4, RG1.6, RG2.4, RG3.1, RE2.1, RE2.2, RE3.2	IT risk management methods
RG2.4, RR3.4	IT risk management process monitoring methods

Inputs y Outputs

Los 9 procesos del Riesgo de TI a pesar de que se listan secuencialmente, están relacionados de una forma compleja, ya que ellos comparten información y dependen unos de otros.

Los Inputs sugieren que la información de una actividad de riesgo de TI, necesita de otras actividades y procesos para ser exitosa. Consecuentemente las actividades de riesgo de TI generan información (Outputs) para soportar otras actividades y procesos de administración de riesgo empresarial y de gobierno de TI.

Información por Proceso

MANAGEMENT GUIDELINES—RG1

RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG1.1 Develop an enterprise-specific IT risk management framework.	A	R	R	R	C	I	R	I	C	I	C
RG1.2 Develop IT risk management methods.	C	C	A	R	C	I	C	C	C	I	C
RG1.3 Perform an enterprise-wide IT risk assessment.	I	A	R	R	C	I	R	C	R	C	C
RG1.4 Propose IT risk tolerance thresholds.	I	I	C	R	C	I	A	C	C		C
RG1.5 Approve IT risk tolerance.	A	C	C	C	C	R	C	C	C	C	C
RG1.6 Align policy and standards statements with IT risk tolerance.		I	A	R	I	C	R	I	C	R	I
RG1.7 Promote an IT risk-aware culture.	A	R	R	R	R	R	R	R	R	R	R
RG1.8 Promote effective communication of IT risk.	A	R	R	I	I	R	I	I	I	I	C

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

Información por Proceso

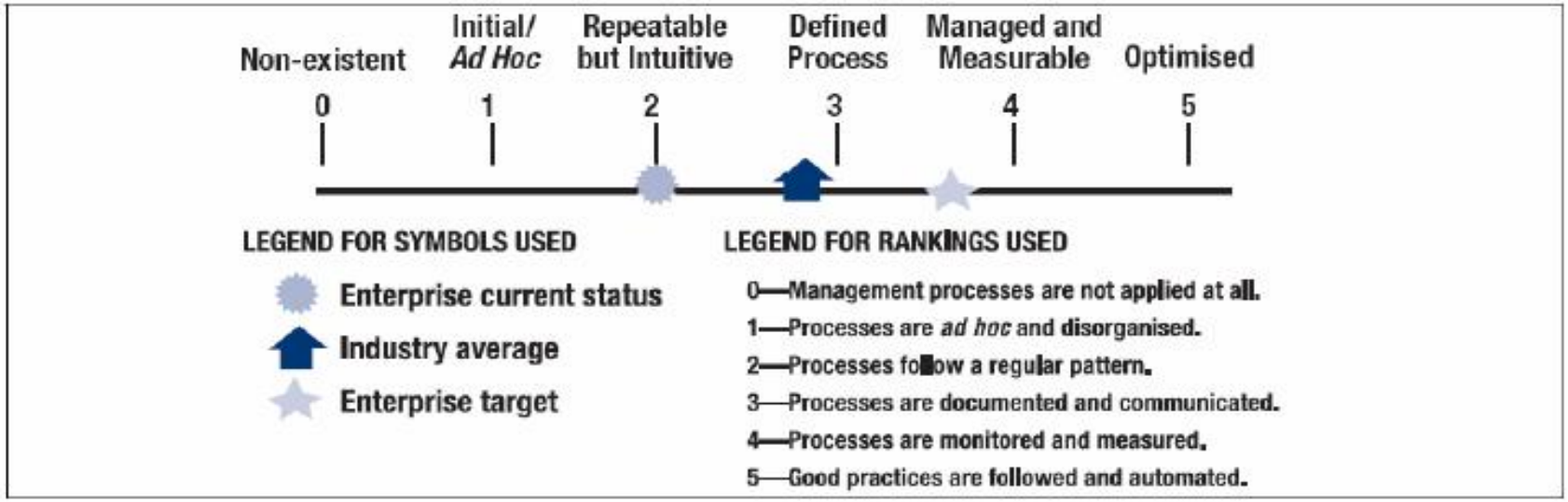
RG1 Establish and Maintain a Common Risk View Risk Governance

Goals and Metrics

Activity Goals	Process Goal	RG Goal
• Develop an enterprise-specific IT risk management framework. • Develop IT risk management methods. • Perform an enterprise-wide IT risk assessment. • Propose IT risk tolerance thresholds. • Approve IT risk tolerance. • Align policy and standards statements with IT risk tolerance. • Promote an IT risk-aware culture. • Promote effective communication of IT risk.	• Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Existence of a defined and documented IT risk management framework • Degree of completeness of the IT risk management framework • Percentage of the IT risk management framework covered by defined methods • Percentage of IT risk management structures and activities set up vs. planned • Frequency of enterprise-wide IT risk assessments • Level of executive participation in enterprise-wide IT risk assessments (e.g., attend in person, send a subordinate, receive report) • Number of out-of-cycle enterprise-wide IT risk assessments • Number of aligned policies to which intended audience has signed adherence • Extent to which risk management communications and training are targeted to specific roles and responsibilities	• Number of known executive-level risk tolerance violations not subjected to disciplinary action (enforcement of policy) • Number of IT-related events with business impact in which a failure to escalate was a factor in event occurrence and/or the loss magnitude (e.g., the risk manager did not know or there was an impaired cultural ability to escalate) • Number of policies in force with one or more statements contradicting a related risk tolerance (alignment of IT policies with tolerance) • Number of IT risk issues that exceed risk tolerance	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

Información por Dominio

—Maturity Model



Información por Dominio

Domain Maturity Model (RG)
High-Level

0 Non-existent when
The enterprise does not recognise the need to consider the business impact from IT risk. Decisions involving IT risk taking tend to be based on lack of information or incorrect information. There is no awareness of external requirements for IT risk management and integration with enterprise risk management.

1 Initial when
There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any IT risk identification criteria vary widely across the enterprise and the IT organisation. By default, IT is accountable for problem management, availability, system access, etc. Risk appetite and tolerance are considered only during episodic risk assessments. Enterprise policies and standards, which are minimal at best, may be incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. IT risk management skills may exist on an *ad hoc* basis, but they are not actively developed. *Ad hoc* control-centric inventories are dispersed across desktop applications.

2 Repeatable when
There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed. Risk tolerance is set locally and may be difficult to aggregate. Investments are focused on specific risk issues within functional and business silos (e.g., security, business continuity, operations). There is board-issued guidance for risk management. Minimum skill requirements, which include an

Información por Dominio

Risk Governance (RG) Detailed Maturity Model (Part 1)			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to consider the business impact from IT risk. Decisions involving IT risk taking tend to be based on lack of information or incorrect information. There is no awareness of external requirements for IT risk management and integration with enterprise risk management.		
1	There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any IT risk identification criteria vary widely across the enterprise and the IT organisation. IT risk issues are primarily communicated by assurance groups (e.g., internal audit). Minimal structure and basis for discussion of IT risk concepts exist. Senior managers and IT executives struggle with IT risk language.	By default, IT is accountable for problem management, availability, system access, etc. Ownership of IT risk in the context of business services and processes is not defined. There is no consideration of business accountability and responsibility for proactive IT risk management. No linkage to an individual performance measurement and reward programme exists. There is no business expectation of value from including IT executives in risk decisions.	Risk appetite and tolerance are considered only during episodic risk assessments. Investments are focused on externally imposed requirements and expectations. Reporting is compliance-driven and focused on remediation of issues identified by assurance groups and external parties.
2	There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. Some localised IT understanding of risk/reward exists. Senior managers and IT executives are developing a common language for IT risk, but IT risk discussions across silos may be impaired by competing business unit and function-specific risk language.	There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed. The enterprise risk committee charter covers IT risk, but IT has minimal representation. Performance targets are tied to meeting external reporting requirements and minimising negative findings. Roles are only partially defined and contain overlaps (e.g., risk evaluation overlaps with risk response, IT implementers are empowered to prescribe and opine). There is confusion about responsibility for integrating IT risk management with operations and enterprise risk management. When problems occur, a culture of blame tends to exist.	Risk tolerance is set locally and may be difficult to aggregate. Investments are focused on specific risk issues within functional and business silos (e.g., security, business continuity, operations). Regular manual reporting of IT risk management activities is directed to local IT management.
3	IT people generally understand how IT-related failures or events impact enterprise objectives and cause direct or indirect loss to the enterprise, while business people generally understand how IT-related failures or events can affect key services and processes. 	There is a designated leader for IT risk across the enterprise who is engaged with the enterprise risk committee, where IT risk is in scope and discussed. The business understands how IT fits in the enterprise-wide, or portfolio view, risk perspective. The IT risk leader has a strong relationship with the CFO and is regularly consulted during portfolio management and	Enterprise risk tolerance is derived from local tolerances, and IT risk management activities are being aligned across the enterprise. Investments are being made against common risk issues although they may not address the root cause in all cases.

Información por Dominio

Risk Governance (RG) Detailed Maturity Model (Part 2)			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
0			
1	Enterprise policies and standards, which are minimal at best, may be incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. Minimal procedures for IT risk management exist. Policies and standards are not kept up to date relative to evolving business, technology or threat landscapes.	IT risk management skills may exist on an *ad hoc* basis, but they are not actively developed. Enterprise risk managers and business process owners lack IT risk understanding. IT personnel lack an understanding of the business impact of IT risk.	*Ad hoc* control-centric inventories are dispersed across desktop applications. Policies and standards exist in multiple formats. There is no workflow around incidents and risk decisions.
2	There is board-issued guidance for risk management. Policies and standards are established for functional and business silos and may not align with the board guidance and overall business risk appetite.	Minimum skill requirements, which include an awareness of IT risk, are identified for critical enterprise risk areas. Risk awareness training focuses on policy and some risk language. IT risk management training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	Functional and IT silo-specific inventories of risk issues exist. Key elements of risk decisions are recorded in desktop applications. Some desktop-based risk management tools may exist, but a co-ordinated approach and expected benefits from tools are lacking.
3	Formal risk categories have been identified and described in clear terms. Enterprise policies and standards reflect overall business risk appetite. Established risk policy is based on board guidance. Important issues are directed to senior management. The process, policies and procedures are defined and documented for all key IT risk management activities. Exceptions are resolved in a formal manner.	Skill requirements are defined and documented for all enterprise risk areas and include IT risk concepts. Risk awareness training includes situations and scenarios beyond specific policy and the structures and a common language for communicating risk. Enterprise risk managers and business process owners receive targeted IT training, e.g., IT for finance executives. IT personnel receive training on business activities, products, general business risk, competing risk issues and business dependency on IT. A formal training plan has been developed.	Requirements are defined for a centralized inventory of risk issues. Workflow tools are used to escalate risk issues and track decisions. Data collection tools can distinguish amongst multiple event types.

Comentarios y Conclusiones

- Si bien existen diversas metodologías para llevar a cabo una adecuada administración de riesgos a nivel empresarial, son pocas las que involucran el efecto de los riesgos de TI en la organización y menos aún, las que integran y relacionan actividades de identificación, gobierno y administración de los riesgos de TI.

- Este Marco de Riesgos de TI complementa muy bien a COBiT, ya que mientras COBiT establece buenas prácticas como el ***medio*** para la administración de riesgo, el Marco de Riesgos de TI (The Risk IT Framework) establece buenas prácticas para el ***fin***.

- El documento al que hace referencia esta presentación, puede constituir una herramienta con las que todos los profesionales relacionados con el Gobierno de TI, puedan promover en sus organizaciones o las de sus clientes, la importancia que tiene una administración efectiva de los riesgos de TI y su relación con la buena marcha del negocio.

Riesgo Empresarial:
Identificación, Gobierno y Administración del Riesgo de TI

El Marco de Riesgo de TI

Edmundo Treviño Gelover,
CGEIT, CISM, CISA