



8 avril 2010

Jean-Louis Bleicher

Le management des risques : un juste équilibre

- « Menace qu'un événement, une action ou une absence d'action affecte la capacité d'une organisation à maximiser sa valeur et à atteindre ses objectifs. Le risque provient aussi bien des opportunités ratées que des menaces potentielles. » *norme AS/NZS 4360 sur le Risk Management (1999-2004)*
- **Risque et valeur sont les deux faces d'une même pièce**
- Toute initiative comporte un risque, mais...à vouloir éliminer tous les risques on peut rater des opportunités de générer de la valeur
- Il faut donc rechercher un juste équilibre...d'autant plus que le risque zéro n'existe pas

Pourquoi s'intéresser aux risques informatiques ?

- Toutes les entreprises dépendent fortement de leurs SI
- Les entreprises comme les SI sont en évolution constante
- Le risque informatique est un risque opérationnel majeur mais difficile à gérer
- Les métiers sont les premiers concernés par le risque informatique
- Il est important d'intégrer le management des risques informatiques aux pratiques existantes de management des risques

SI = Système d'Information + Système Informatique

Risk IT

- Risk IT est le premier guide relatif aux risques informatiques à donner une vision complète des **risques métiers liés à l'informatique**
- Risk IT aide les entreprises à gérer leurs risques pour atteindre leurs objectifs, saisir les opportunités et rechercher un meilleur résultat
- Bien que basé sur COBIT et le prolongeant, Risk IT constitue à lui seul un excellent référentiel
- **Risk IT facilite l'intégration d'autres normes** et pratiques de management des risques génériques ou spécifiques à un domaine
- Risk IT a été réalisé au sein de l'ISACA par des volontaires qui réalisent des guides « vivants »

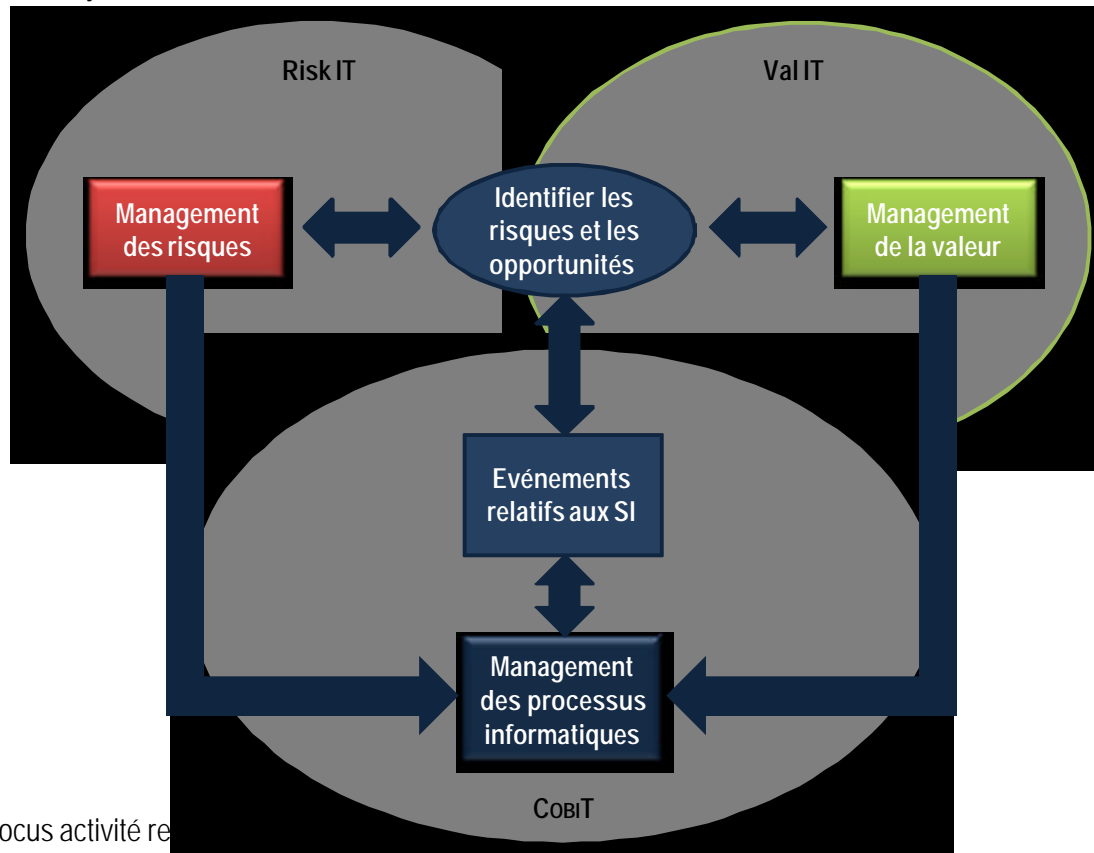
Le risque informatique est un risque métier

- Pour exprimer le risque informatique en termes métiers
Risk IT s'appuie sur plusieurs modèles :
 - COBIT : critères d'information (efficacité, efficience, confidentialité, intégrité, disponibilité, conformité, fiabilité)
 - Tableau de bord prospectif détaillé : finance, client, processus internes, apprentissage et croissance
 - Westerman (IT Risk: Turning Business Threats into Competitive Advantage) : agilité, exactitude, accès, disponibilité
 - COSO ERM : stratégie, opérations, rapports, conformité
 - FAIR (Factor Analysis of Information Risk) : productivité, coût de traitement, coût de remplacement, avantage concurrentiel, juridique, réputation

Risk IT élargit COBIT et Val IT

- Risk IT complète et élargit COBIT et Val IT permettant ainsi de disposer d'un ensemble de ressources plus complet sur la gouvernance des SI

Focus objectif métier – *confiance et valeur*



Focus activité réelle

Management des risques informatiques

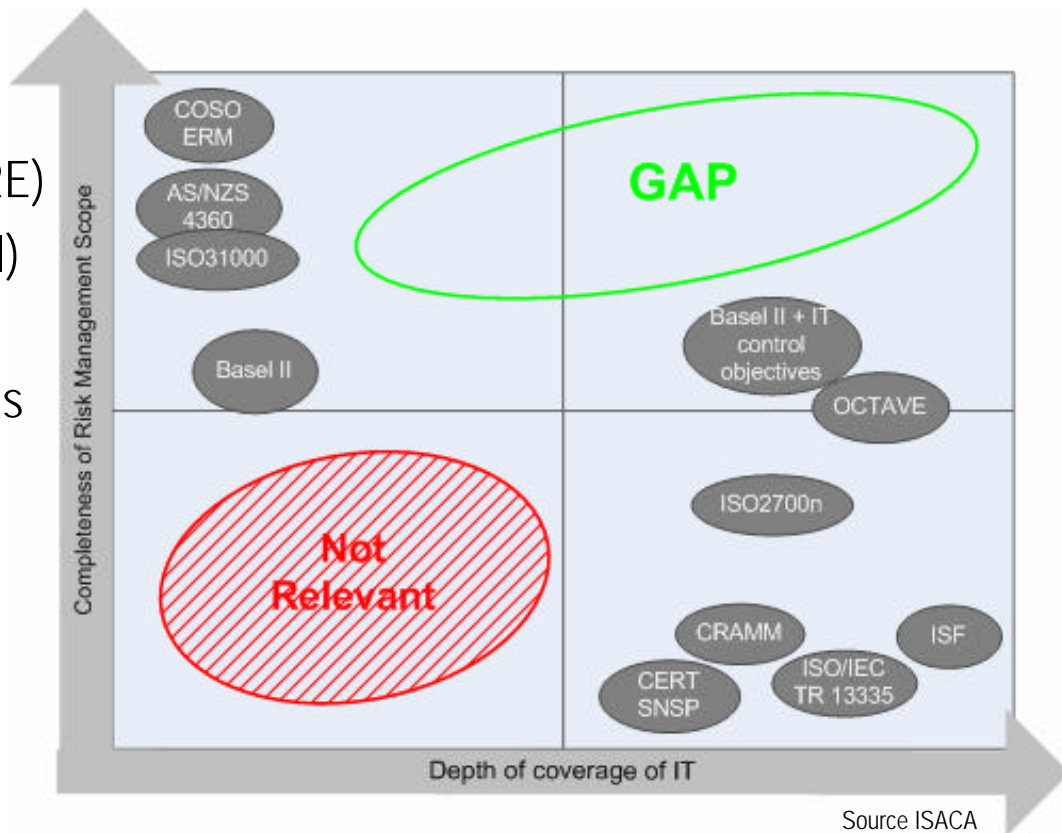
- Risk IT ne se limite pas à la sécurité de l'information. Il couvre **tous** les risques informatiques dont :
 - La livraison des projets en retard
 - Le manque de valeur apportée par les SI
 - La non-conformité
 - Le défaut d'alignement
 - L'obsolescence ou le manque de flexibilité des architectures informatiques
 - Les problèmes liés à la délivrance de services

Unique sur la Place

- Risk IT fournit une vision équilibrée des risques métiers de l'entreprise liés à l'informatique :
 - Rassemble tous les aspects des risques informatiques, dont les notions de valeur, changement, disponibilité, sécurité, projets et continuité
 - Etablit le lien avec les concepts de management des risques de l'entreprise et les modèles comme COSO ERM, ARMS et ISO 31000
 - Complète les autres normes et référentiels trop génériques (c.à.d. orientés MRE – Management des Risques de l'Entreprise) ou trop centrés sur un sujet (par exemple, sécurité de l'information- SSI)
 - Offre une vision unique et complète des risques métiers inhérents à l'informatique qui peuvent coûter aux entreprises des millions d'euros de pertes de revenus ou d'opportunités

Où se situe Risk IT ?

- Il existe des normes et des référentiels ...mais trop
 - Génériques (orientés MRE)
 - Spécifiques (orientés SSI)
- Jusqu'à présent il n'y avait pas de référentiel global sur le management des risques informatiques
- Risk IT comble ce trou



Qu'apporte Risk IT ?

- Aide les responsables et le management à se poser les questions clés, à prendre de meilleures décisions en tenant compte des risques, et à s'assurer que le risque informatique est géré de manière effective dans leur entreprise
- Permet de gagner du temps, de réaliser des économies et de limiter l'effort grâce à des outils pour traiter les risques métiers
- Intègre le management des risques métiers liés à l'informatique au MRE global
- Aide le leadership à comprendre l'appétence et la tolérance aux risques
- Fournit un guide de bonnes pratiques dictées par les besoins des dirigeants d'entreprise partout dans le monde

Risk IT : pour qui ?

- Toutes les entreprises utilisatrices de l'informatique, de l'entreprise individuelle à la multinationale
- Adaptable à tout type d'entreprise partout dans le monde
- Plus particulièrement destiné aux :
 - CA et Directions Générales
 - Responsables de la gestion des risques de l'entreprise et responsables des risques opérationnels
 - Directions informatiques et responsables informatiques
 - Régulateurs
 - RSSI
 - Responsables de la gouvernance de l'entreprise
 - Responsables métiers
 - Auditeurs internes et externes

Risk IT répond aux besoins des praticiens

- **Besoins fonctionnels**

- Établit le lien avec les modèles de management des risques métiers
- Utilise un modèle de processus performant orienté métier de A à Z
- Permet l'intégration des silos de management des risques informatiques

- **Besoins de facilité d'utilisation**

- Guide pratique utilisable seul ; complète COBIT et Val IT
- Modèle de processus continu, étayé par par des modèles de maturité et des outils
- Comprend un référentiel et un guide de bonnes pratiques

Contenu de Risk IT

- **Le Référentiel Risk IT**
 - Comprend une synthèse et les fondements du référentiel
 - Fournit de l'information sur l'univers des risques, les processus et les activités prioritaires
- **Le guide du praticien Risk IT**
 - Guide pratique de mise en place du management des risques informatiques

Les six principes directeurs de Risk IT

- Toujours se rattacher aux objectifs métiers
- Aligner le management des risques métiers liés à l'informatique sur le MRE global
- Equilibrer les coûts et les bénéfices du management des risques informatiques
- Promouvoir une communication honnête et généreuse sur les risques informatiques
- Donner le juste ton au plus haut niveau en définissant et en imposant la responsabilité de chacun pour fonctionner dans des niveaux de tolérance acceptables et bien définis
- En faire un processus continu et une partie des activités quotidiennes

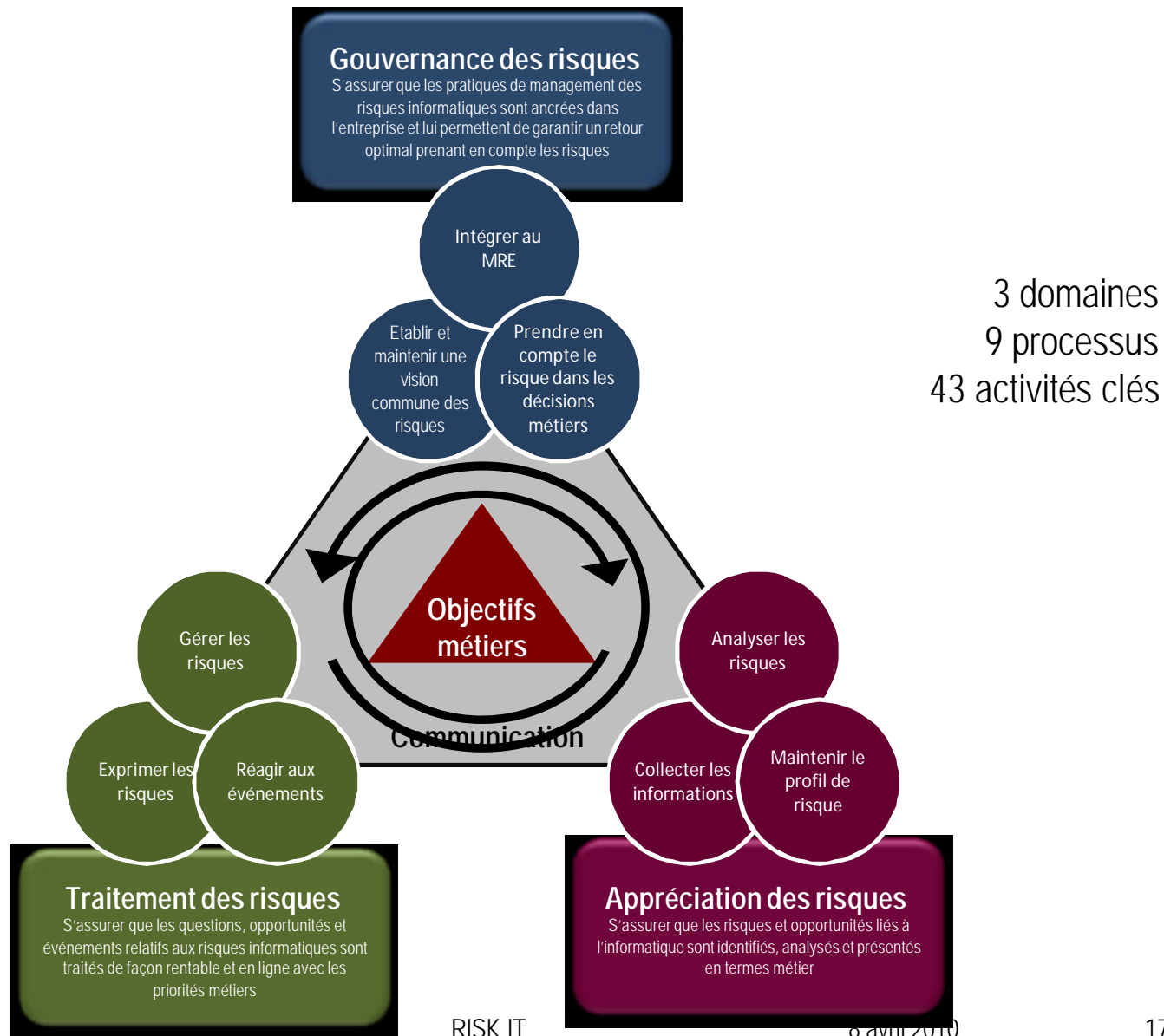
Les trois catégories de risques de Risk IT

- Risques liés à la **génération de valeur/bénéfices** grâce aux SI
 - Opportunités manquées d'utiliser les technologies pour améliorer l'efficacité ou l'efficience des processus métiers ou pour faciliter de nouvelles initiatives métiers
- Risques liés à la **réalisation de programmes/projets** informatiques
 - Contribution des SI à des solutions métiers nouvelles ou améliorées
- Risques liés à la **délivrance de services et à l'exploitation** informatique
 - Performance des systèmes pouvant conduire à la destruction ou réduction de valeur pour l'entreprise

Le Référentiel Risk IT = le quoi

- **L'essentiel du management des risques**
 - Gouvernance des risques : appétence et tolérance au risque, responsabilités et autorité en matière de management des risques informatiques, sensibilisation et communication, culture du risque
 - Appréciation des risques : description des impacts métiers et des scénarios de risque
 - Traitement des risques : ICR (Indicateurs Clés de Risques), traitement et hiérarchisation des risques
- **Façon dont Risk IT complète et enrichit COBIT et Val IT** (rappel : Risk IT peut s'utiliser sans COBIT ou Val IT)
- **Pour chaque processus**
 - Description des activités
 - Tableau des éléments d'entrée/sortie (au niveau activité)
 - Tableau RACI (au niveau activité)
 - Tableau des objectifs et métriques (activité, processus, domaine)
- **Deux modèles de maturité pour chaque domaine**
- **Annexes**
 - Références
 - Tableau comparatif de Risk IT avec les autres normes et référentiels de management des risques
 - Glossaire

Les trois domaines de Risk IT



3 domaines
9 processus
43 activités clés

Un double modèle de maturité

- Un modèle de synthèse sur une échelle à 6 niveaux : inexistant, initialisé, reproductible, défini, géré, optimisé
- Un modèle détaillé, sur la même échelle à 6 niveaux, par grand thème :
 - Sensibilisation et communication
 - Responsabilité et autorité
 - Fixation et mesure des objectifs
 - Politiques, normes et procédures
 - Compétences et expertise
 - Outils et automatisation

Exemple d'activité et de modèle de maturité détaillé

THE RISK IT FRAMEWORK

RG3.4 Accept IT risk.

Using the established IT risk tolerance thresholds as a guide, decide whether to accept the remaining risk exposure level. Consider relevant information from risk analysis reports such as loss probabilities and ranges, risk response options, cost/benefit expectations, and the potential effects of risk aggregation. Discuss with impacted business process owners and together examine the risk-return ratios, and determine where to spend the risk budget on 'known' risks to allow acceptance of the unknown risk. Obtain business agreement on risk acceptance or, if no acceptance, the appropriate risk response requirements. Document how risk was considered in the decision and the rationale for any exceptions to risk tolerance (e.g., significant strategic business opportunity). Ensure that risk acceptance decisions and risk response requirements are communicated across organisational lines in accordance with established enterprise risk and corporate governance policies and procedures.

From	Inputs	To	Outputs
RG1.3	IT risk tolerance thresholds	RG2.1, RE2.3, RR2.1, RR2.3, RR2.4	Risk response requirements
RG2.2	Integrated risk management strategy	RG2.5, RE3.5, RE3.6	Documented acceptance of risk
RG3.2	Approved risk analysis report, risk analysis limitations	RE2.1	Risk analysis request
RE3.5	IT risk profile	RE3.5	IT risk profile changes
RR1.1	Loss/gain probabilities and ranges, risk response options, cost/benefit expectations		
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities		
RR1.2, RR2.2	Control gaps and policy exceptions		
RR1.3	Independent IT assessment findings in context, vulnerability events		
RR2.2	Risk aggregation data		

RG3.5 Prioritise IT risk response activities.

Examine the portfolio of risk response activities to identify those with a greater probable impact on overall risk reduction. Quantify the overall expected effect on the probable frequency and magnitude of related risk scenarios through the planned application of controls, capability and resources. Based on dimensions such as current risk level and effectiveness/cost ratio, classify and balance responses (e.g., quick wins, opportunities, deferred efforts) with those that may need a business case. Emphasise specific projects with relatively greater odds to:

- Reduce risk concentrations (e.g., improvements to architecture, separation of operational units and systems)
- Implement controls that directly address multiple risk types and are cost effective
- Implement controls that improve process effectiveness and prevent excessive risk taking

Record the rationale, constraints and how the decision is driving changes to published policy, operational controls, capabilities, resource deployments and communication plans. When applicable, record the rationale for exceeding or falling below risk appetite and tolerance.

From	Inputs	To	Outputs
RG1.3	IT risk tolerance thresholds	RE2.1	Risk analysis request
RG3.2	Approved risk analysis report, risk analysis limitations	RE3.5	IT risk profile changes
RE3.5	IT risk profile	RE3.5, RR2.3	Risk response priority (risk disposition)
RR1.1	Loss/gain probabilities and ranges, risk response options, cost/benefit expectations	RR2.3; Val IT PM4 (if a full business case is already made), IM1 (if a business case still needs to be made)	Risk management benefits assigned to IT portfolio
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities		
RR1.3	Independent IT assessment findings in context, vulnerability events		
Val IT V63	Investment evaluation criteria		
Val IT IM2	Complete understanding of candidate programmes including alternative courses of action		
Cost P05	IT budgets		
*	Operating budget		

* Input from/output to outside Risk IT, Val IT and Cost

THE RISK IT FRAMEWORK

Figure 28—RG Detailed Maturity Model Part 1 (cont.)

	Awareness and Communication	Responsibility and Accountability	Goal Setting and Measurement
4	<p>Risk culture is analysed and reported. The business understands IT risk/reward. IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood.</p> <p>The IT risk language spoken by senior executives is blending and aligning with corporate risk language. IT risk discussions are a normal part of executive decision making.</p>	<p>The designated leader for IT risk across the enterprise is fully engaged with the enterprise risk committee, which expects value from including IT in decisions.</p> <p>The IT department's role in operational risk management and the broader ERM is well understood. Integrated risk management is embedded in strategic planning and business operations.</p> <p>All IT risk domains have a nominated owner, and responsibility and accountability are accepted. Senior business management and IT management together determine the acceptable level of risk that the enterprise will tolerate. A reward culture that motivates positive action is in place.</p>	<p>The board defines risk appetite and tolerance across the risk universe, including IT risk. Risk tolerance may be refined by the enterprise risk committee or an IT risk council. Risk portfolio views are dynamic, and risk tolerance is evaluated based on different views. Better investment decisions result from enterprise visibility into costs, IT risk issues and benefits/rewards.</p> <p>Opportunities associated with risk are part of the risk plan's expected outcomes.</p> <p>Investments are balanced against a portfolio view of risk and address the root cause.</p> <p>Regular reporting of business outcomes related to IT risk management is made to business management.</p>
5	<p>Senior executives make a point of considering all aspects of IT risk in their decisions.</p> <p>The enterprise views integrated risk management as a source of business value.</p>	<p>The IT risk leader is considered a trusted advisor during design, implementation and steady-state operations. Executive sponsorship is strong, and the tone from the top has embedded integrated risk management into the enterprise culture. Roles and responsibilities are process-driven, with cross-functional teams collaborating. Accountability for risk management to help achieve objectives is embedded in all processes, support functions, business lines and geographic locations.</p> <p>The IT department is a major player in business-line operational risk efforts and enterprise risk efforts.</p>	<p>Strategic objectives are based on an executive-level understanding of IT-related business threats, risk scenarios and competitive opportunities.</p> <p>The enterprise employs robust business analytics to measure the effectiveness of managing uncertainties and seizing timely opportunities.</p>

Figure 29—RG Detailed Maturity Model Part 2 (a)

	Policies, Standards and Procedures	Skills and Expertise	Tools and Automation
0			
1	<p>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.</p> <p>Minimal procedures for IT risk management exist.</p> <p>Policies and standards are not kept up to date relative to evolving business, technology or threat landscapes.</p>	<p>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.</p>	<p>Ad hoc inventories of controls that are unrelated to risk are dispersed across desktop applications. Policies and standards exist in multiple formats. There is no workflow around incidents and risk decisions.</p>
2	<p>There is board-issued guidance for risk management.</p> <p>Policies and standards are established for functional and business silos and may not align with the board guidance and overall business risk appetite.</p>	<p>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.</p> <p>IT risk management training is provided in response to needs, rather than on the basis of an agreed-upon plan, and informal training on the job occurs.</p>	<p>Functional and IT silo-specific inventories of risk issues exist.</p> <p>Key elements of risk decisions are recorded in desktop applications.</p> <p>Some desktop-based risk management tools may exist, but a co-ordinated approach and expected benefits from tools are lacking.</p>

Le Guide du Praticien Risk IT : le comment

- Revue détaillée du modèle de processus Risk IT
- Risk IT par rapport à COBIT et Val IT
- Comment l'utiliser :
 - Définir l'univers des risques et cadrer le management des risques
 - Appétence et tolérance au risque
 - Sensibilisation, communication et rapports sur les risques : dont les Indicateurs Clés de Risque, le profil de risque, la consolidation des risques et la culture du risque
 - Exprimer et décrire les risques : guide sur le contexte métier, la fréquence, l'impact, les objectifs métiers de COBIT, la cartographie des risques, le registre des risques
 - Les scénarios de risque (36) : dont les facteurs de risque liés à la capacité et à l'environnement
 - Le traitement des risques et leur hiérarchisation
 - Un modèle d'analyse de risque : diagramme en colonne et par acteur
 - Réduction des risques en utilisant COBIT et Val IT (pour les 36 scénarios)
- Cartographie de Risk IT par rapport aux autres normes et référentiels de management des risques
- Glossaire

Extrait du Guide du praticien (scénario et réduction)

5. RISK SCENARIOS

Risk Scenario Components	Risk Consequence		Risk	
	IT Operations or Service Delivery	IT Performance and Impact Delivery	IT Operations or Service Delivery	IT Performance and Impact Delivery
High Level Risk Scenario	IT Service Quality	IT Service Availability	IT Service Quality	IT Service Availability
15. Project quality	Internal	Internal	Internal	Internal
16. Shortfall in performance of IT service suppliers	Internal	Internal	Internal	Internal
17. Insecure data theft	Internal/External	Internal	Internal	Internal
18. Destruction of infrastructure	Internal/External	Internal	Internal	Internal
19. Ineffective data backup	Internal	Internal	Internal	Internal
20. Failure of IT service suppliers	Internal	Internal	Internal	Internal
21. Ineffective data backup	Internal	Internal	Internal	Internal
22. Failure of IT service suppliers	Internal	Internal	Internal	Internal
23. Ineffective data backup	Internal	Internal	Internal	Internal
24. Failure of IT service suppliers	Internal	Internal	Internal	Internal
25. Ineffective data backup	Internal	Internal	Internal	Internal
26. Failure of IT service suppliers	Internal	Internal	Internal	Internal
27. Ineffective data backup	Internal	Internal	Internal	Internal
28. Failure of IT service suppliers	Internal	Internal	Internal	Internal
29. Ineffective data backup	Internal	Internal	Internal	Internal
30. Failure of IT service suppliers	Internal	Internal	Internal	Internal
31. Ineffective data backup	Internal	Internal	Internal	Internal
32. Failure of IT service suppliers	Internal	Internal	Internal	Internal
33. Ineffective data backup	Internal	Internal	Internal	Internal
34. Failure of IT service suppliers	Internal	Internal	Internal	Internal
35. Ineffective data backup	Internal	Internal	Internal	Internal
36. Failure of IT service suppliers	Internal	Internal	Internal	Internal
37. Ineffective data backup	Internal	Internal	Internal	Internal
38. Failure of IT service suppliers	Internal	Internal	Internal	Internal
39. Ineffective data backup	Internal	Internal	Internal	Internal
40. Failure of IT service suppliers	Internal	Internal	Internal	Internal
41. Ineffective data backup	Internal	Internal	Internal	Internal
42. Failure of IT service suppliers	Internal	Internal	Internal	Internal
43. Ineffective data backup	Internal	Internal	Internal	Internal
44. Failure of IT service suppliers	Internal	Internal	Internal	Internal
45. Ineffective data backup	Internal	Internal	Internal	Internal
46. Failure of IT service suppliers	Internal	Internal	Internal	Internal
47. Ineffective data backup	Internal	Internal	Internal	Internal
48. Failure of IT service suppliers	Internal	Internal	Internal	Internal
49. Ineffective data backup	Internal	Internal	Internal	Internal
50. Failure of IT service suppliers	Internal	Internal	Internal	Internal
51. Ineffective data backup	Internal	Internal	Internal	Internal
52. Failure of IT service suppliers	Internal	Internal	Internal	Internal
53. Ineffective data backup	Internal	Internal	Internal	Internal
54. Failure of IT service suppliers	Internal	Internal	Internal	Internal
55. Ineffective data backup	Internal	Internal	Internal	Internal
56. Failure of IT service suppliers	Internal	Internal	Internal	Internal
57. Ineffective data backup	Internal	Internal	Internal	Internal
58. Failure of IT service suppliers	Internal	Internal	Internal	Internal
59. Ineffective data backup	Internal	Internal	Internal	Internal
60. Failure of IT service suppliers	Internal	Internal	Internal	Internal
61. Ineffective data backup	Internal	Internal	Internal	Internal
62. Failure of IT service suppliers	Internal	Internal	Internal	Internal
63. Ineffective data backup	Internal	Internal	Internal	Internal
64. Failure of IT service suppliers	Internal	Internal	Internal	Internal
65. Ineffective data backup	Internal	Internal	Internal	Internal
66. Failure of IT service suppliers	Internal	Internal	Internal	Internal
67. Ineffective data backup	Internal	Internal	Internal	Internal
68. Failure of IT service suppliers	Internal	Internal	Internal	Internal
69. Ineffective data backup	Internal	Internal	Internal	Internal
70. Failure of IT service suppliers	Internal	Internal	Internal	Internal
71. Ineffective data backup	Internal	Internal	Internal	Internal
72. Failure of IT service suppliers	Internal	Internal	Internal	Internal
73. Ineffective data backup	Internal	Internal	Internal	Internal
74. Failure of IT service suppliers	Internal	Internal	Internal	Internal
75. Ineffective data backup	Internal	Internal	Internal	Internal
76. Failure of IT service suppliers	Internal	Internal	Internal	Internal
77. Ineffective data backup	Internal	Internal	Internal	Internal
78. Failure of IT service suppliers	Internal	Internal	Internal	Internal
79. Ineffective data backup	Internal	Internal	Internal	Internal
80. Failure of IT service suppliers	Internal	Internal	Internal	Internal
81. Ineffective data backup	Internal	Internal	Internal	Internal
82. Failure of IT service suppliers	Internal	Internal	Internal	Internal
83. Ineffective data backup	Internal	Internal	Internal	Internal
84. Failure of IT service suppliers	Internal	Internal	Internal	Internal
85. Ineffective data backup	Internal	Internal	Internal	Internal
86. Failure of IT service suppliers	Internal	Internal	Internal	Internal
87. Ineffective data backup	Internal	Internal	Internal	Internal
88. Failure of IT service suppliers	Internal	Internal	Internal	Internal
89. Ineffective data backup	Internal	Internal	Internal	Internal
90. Failure of IT service suppliers	Internal	Internal	Internal	Internal
91. Ineffective data backup	Internal	Internal	Internal	Internal
92. Failure of IT service suppliers	Internal	Internal	Internal	Internal
93. Ineffective data backup	Internal	Internal	Internal	Internal
94. Failure of IT service suppliers	Internal	Internal	Internal	Internal
95. Ineffective data backup	Internal	Internal	Internal	Internal
96. Failure of IT service suppliers	Internal	Internal	Internal	Internal
97. Ineffective data backup	Internal	Internal	Internal	Internal
98. Failure of IT service suppliers	Internal	Internal	Internal	Internal
99. Ineffective data backup	Internal	Internal	Internal	Internal
100. Failure of IT service suppliers	Internal	Internal	Internal	Internal

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 4B—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)					
Essential Control	Control Reference	Control Title	COBIT Control Objectives/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
1. IT programme selection (cont.)					
Yes	PO5	PO5.2	Prioritization Within IT Budget	Medium	High
Yes	AI1	AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	High	Medium
Yes	FM4	FM4.1	Evaluate and Assign Relative Scores to Programme Business Cases	Medium	High
	PO6	PO6.5	Communication of IT Objectives and Direction	Medium	Medium
	FM1	FM1.3	Define an Appropriate Investment Mix	Medium	Medium
	FM4	FM4.2	Create Overall Investment Portfolio View	Medium	Medium
	IM1	IM1.3	Evaluate the Initial Programme Concept Business Case	Medium	Medium
2. New technologies					
Yes	PO3	PO3.1	Technological Planning	High	High
Yes	PO3	PO3.3	Monitor Future Trends and Regulations	High	High
Yes	FM1	FM1.4	Translate the Business Strategy and Goals into IT Strategy and Goals	High	High
	PO2	PO2.1	Enterprise Information Architecture Model	Medium	Medium

Risk IT en synthèse

- Vision précise des risques informatiques actuels et à venir
- Conseils sur la façon de gérer les risques informatiques de A à Z
- Façon de capitaliser sur le système de contrôle interne de l'informatique
- Intégration aux structures de management des risques et de la conformité de l'entreprise
- Langage commun pour faciliter les relations dans l'entreprise
- Promotion de la notion de propriétaire de risques
- Profil de risque complet pour mieux comprendre le risque

AFAI, ISACA et Risk IT

- L'AFAI publiera en 2010 la version française du Référentiel Risk IT, du Guide du Praticien Risk IT et de la boîte à outils Risk IT (permettant par exemple de créer ses propres scénarios de risque)
- L'ISACA met en place une certification spécifique
- L'AFAI proposera une formation au management des risques et réfléchit à un cursus de préparation au CRISC

