Het ISACA RISK IT Framework voor Testers

Omgaan met risico's

Risk Appetite – Onderzoeken – Maatregelen

Wie is Jaap

Ir. J. van der Leer CRISC CGEIT CISA

43 jaar in de IT werkzaam.
22 jaar ervaring in IT kwaliteit en testen
> 100 testtrajecten geleid in de loop der jaren

Vanaf 1992 gecertificeerd bij ISACA.

Jaap ziet het testen primair als een brugfunctie tussen IT en Business. Waarbij de tester continu balanceert tussen wat mogelijk en wat wenselijk is.

Doel van de presentatie:

- Een waarneembare trend in de markt (crisis) is dat klanten eisen dat goedkoper en efficiënter getest wordt.
- Financiële instellingen hechten, door Basel en Solvency gedreven, steeds meer belang aan risico management en risico gebaseerde sturing van de organisatie, processen en projecten.
- RISK IT biedt een alomvattend raamwerk om met risico's in IT om te gaan.
- Toepassen van RISK IT bij testen leidt aanvullend tot een betere aanpak dan Risico Gebaseerd Testen.

Inhoudsopgave

Waar staat ISACA voor?

- ISACA is begonnen 1969 als
  “Information Systems Audit and Control Association”
- De naam bestaat nog, echter niet meer als acroniem.
- De doelstelling is:
  “Trust in and Value from Information Systems”,
  en in Nederland
  “Vertrouwen in en waarde uit informatiesystemen”

- Certificeringen: CISA, CISM, CGEIT, CRISC

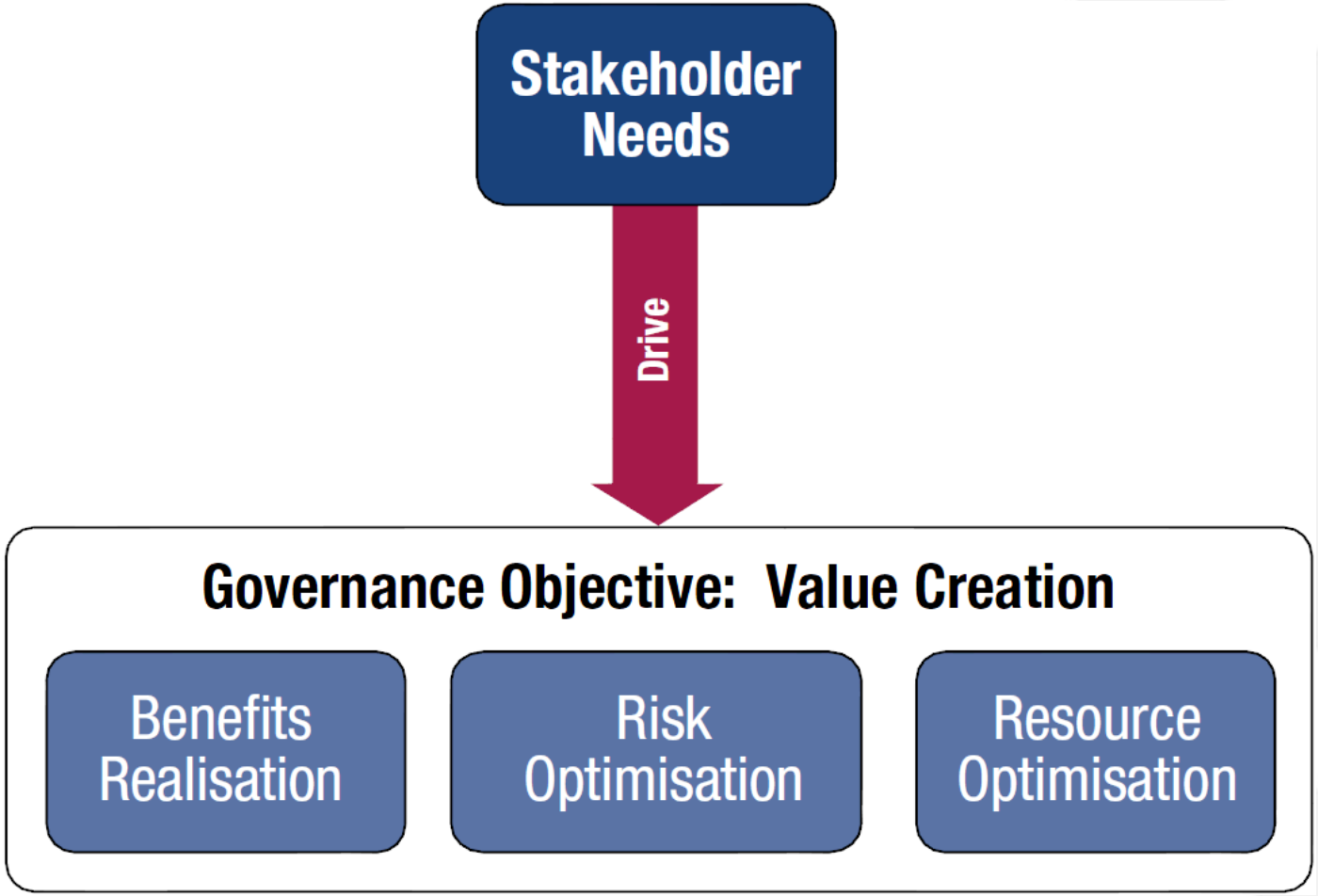
ISACA®
Serving IT Governance Professionals

Wat biedt ISACA?

- Ontzettend veel kennis over hoe ICT aan te sturen, te ontwikkelen, te beheersen, en rendabel te maken.
- Bekende raamwerken ISACA voor haar leden :
  - COBIT, eerste versie 1996, in april 2012 COBIT 5.
  - VAL IT in 2007
  - RISK IT in 2010
- Aanvullende documentatie over hoe de raamwerken te gebruiken, aan te passen en in te voeren.

COBIT 5 – sinds april 2012

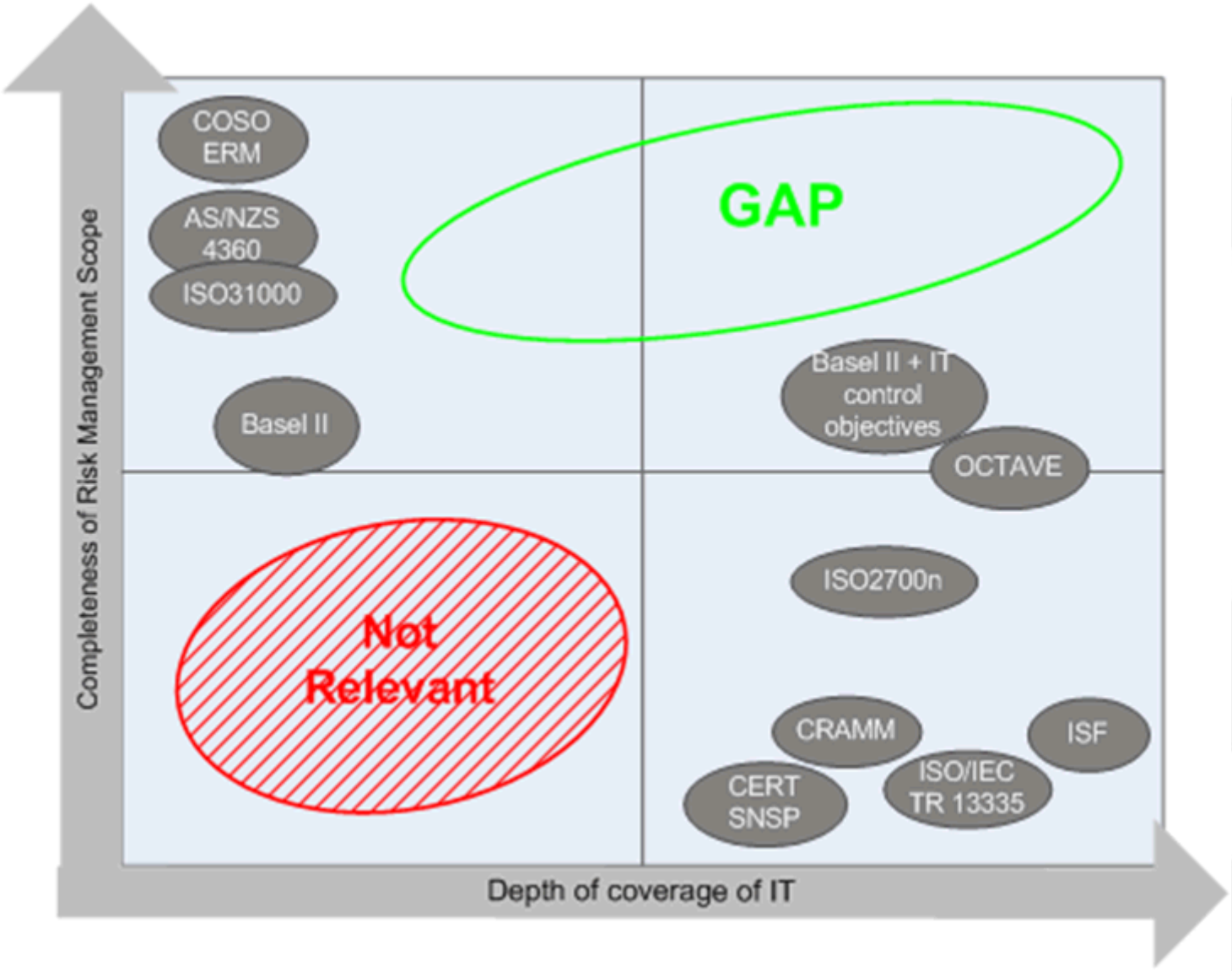
- The one ring that rules them all



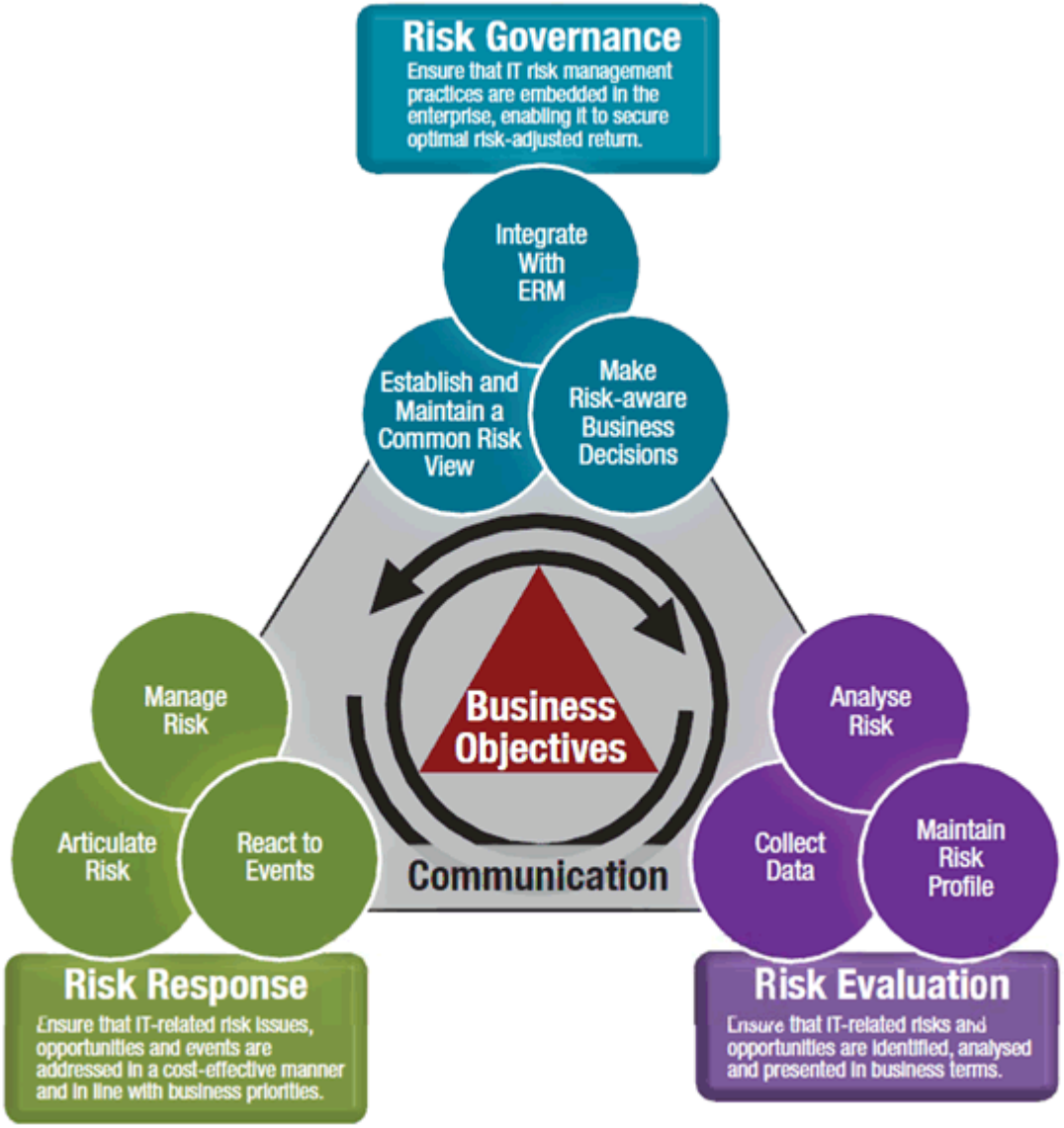
Inhoudsopgave

1. ISACA
2. RISK IT
   - Doel
   - Structuur
3. RISK Appetite
   - Aanvulling op Risk Based Testen
4. Vragen

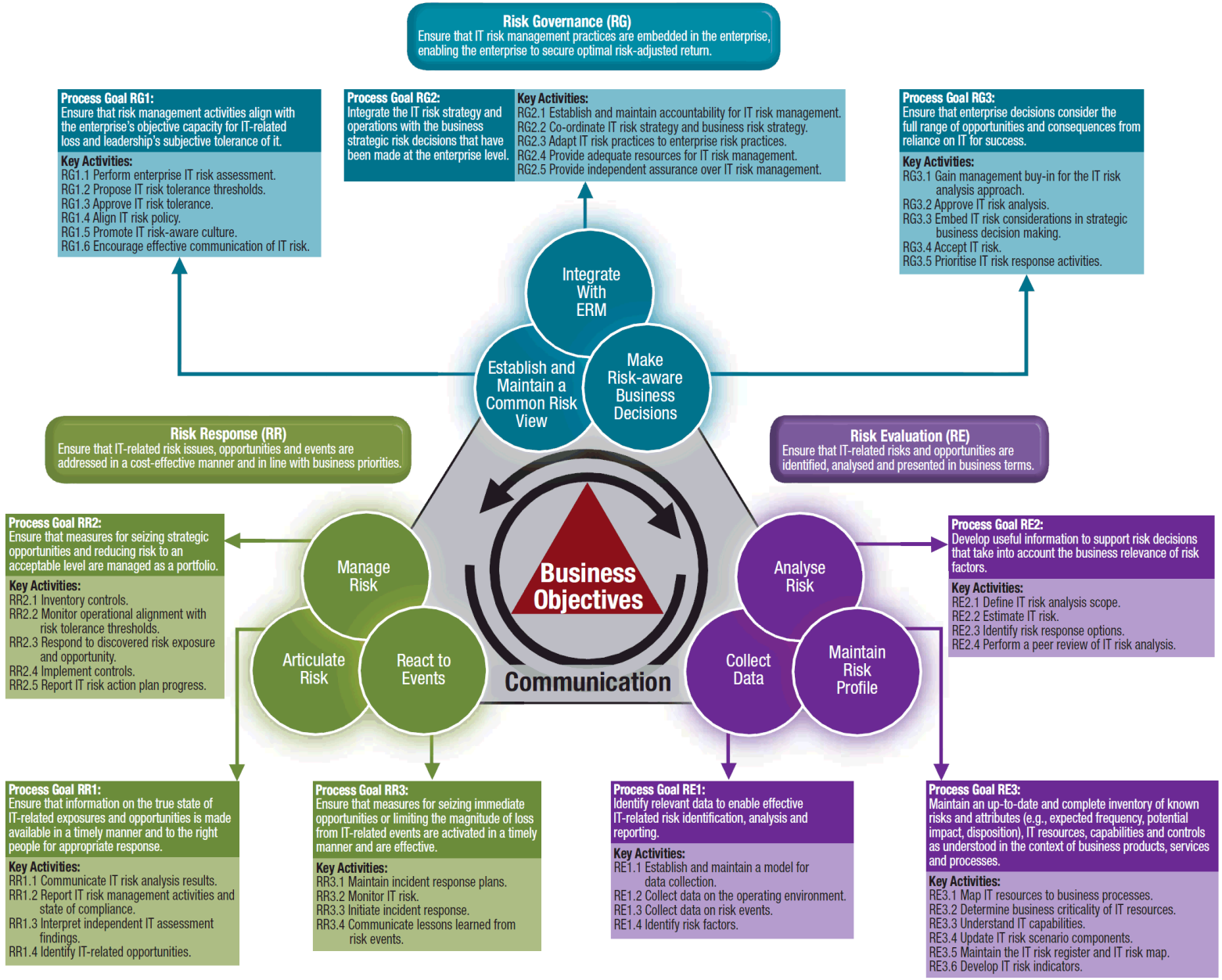
RISK IT: Compleet én IT toegelijk



Drie domeinen van RISK IT:



Aangevuld met activiteiten …



Daarvan voor testen van belang

Process Goal RG1:
Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.

Key Activities:
RG1.1 Perform enterprise IT risk assessment.
RG1.2 Propose IT risk tolerance thresholds.
RG1.3 Approve IT risk tolerance.
RG1.4 Align IT risk policy.
RG1.5 Promote IT risk-aware culture.
RG1.6 Encourage effective communication of IT risk.

Process Goal RE3:
Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.

Key Activities:
RE3.1 Map IT resources to business processes.
RE3.2 Determine business criticality of IT resources.
RE3.3 Understand IT capabilities.
RE3.4 Update IT risk scenario components.
RE3.5 Maintain the IT risk register and IT risk map.
RE3.6 Develop IT risk indicators.

Process Goal RR1:
Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.

Key Activities:
RR1.1 Communicate IT risk analysis results.
RR1.2 Report IT risk management activities and state of compliance.
RR1.3 Interpret independent IT assessment findings.
RR1.4 Identify IT-related opportunities.

Process Goal RE2:
Develop useful information to support risk decisions that take into account the business relevance of risk factors.

Key Activities:
RE2.1 Define IT risk analysis scope.
RE2.2 Estimate IT risk.
RE2.3 Identify risk response options.
RE2.4 Perform a peer review of IT risk analysis.

Testen = Risico's beoordelen.

- Doel: inzicht verschaffen in IT-kwaliteit
  - Ketentesten op Business risico's
  - Nauwe samenwerking met Business management
  - Intense kennis van IT
  - Bijhouden status en bevindingen
  - Rapporteren

Process Goal RE3:
Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.

Key Activities:
RE3.1 Map IT resources to business processes.
RE3.2 Determine business criticality of IT resources.
RE3.3 Understand IT capabilities.
RE3.4 Update IT risk scenario components.
RE3.5 Maintain the IT risk register and IT risk map.
RE3.6 Develop IT risk indicators.

Kunnen we meer met testen?

- Doel: waardevol zijn voor Business, de klant
  - Nauw contact met Business houden, hun taal spreken
  - Ook continuous testing?
  - Alle testen van white box testen tot integrale E2E test integreren?
  - Meedenken over oplossingen
  - Ervaring laten tellen
  - Juridisch ondersteunend

Process Goal RR1:
Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.

Key Activities:
RR1.1 Communicate IT risk analysis results.
RR1.2 Report IT risk management activities and state of compliance.
RR1.3 Interpret independent IT assessment findings.
RR1.4 Identify IT-related opportunities.

Testen, met als basis Risico Analyse

- Doel: met Business risico's en kansen beheersen
  - Systeem-risico's overstijgen naar Business Risico's
  - Risico's ranken volgen Business prioriteiten
  - Bijdrage van testers: deskundig op IT gebied
  - Early warning

Process Goal RE3:
Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.

Key Activities:
RE3.1 Map IT resources to business processes.
RE3.2 Determine business criticality of IT resources.
RE3.3 Understand IT capabilities.
RE3.4 Update IT risk scenario components.
RE3.5 Maintain the IT risk register and IT risk map.
RE3.6 Develop IT risk indicators.

Testen, de Risico Analyse overstijgen

- Doel: aanhaken bij Risico Beleid van de onderneming
  - Vraagt een andere blik op omgaan met Risico's
  - Meer waarde voor de Business tegen lagere kosten.

Process Goal RG1:
Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.

Key Activities:
RG1.1 Perform enterprise IT risk assessment.
RG1.2 Propose IT risk tolerance thresholds.
RG1.3 Approve IT risk tolerance.
RG1.4 Align IT risk policy.
RG1.5 Promote IT risk-aware culture.
RG1.6 Encourage effective communication of IT risk.

Maar: Hoe komen we daar?

Beperkingen van traditioneel RBT

- Onduidelijke prioritering van risico's
- Onderscheid tussen product- en procesrisico's
- Geen inzicht in resulterende bedrijfsrisico's
- Testen kan duurder zijn dan het potentiële verlies
- Of, je test dingen en je constateert dat bevindingen wel opgelost kunnen worden, maar dat oplossen zo duur is dat je het niet gaat doen (en maar beter kunt stoppen)
- Of dat het testen zo veel kost dat er geen voldoende budget voor beschikbaar komt.
- Of dat het testen alle budget voor het oplossen opeet.
- Hent u nog aanvullingen?
  Ik zou zo graag een tweede sheet hebben!

“Standaard” PRIMA risicomatrix (voorbeeld)

PRIMA Product Risico Matrix	Project: Optimalisatie Bestuurs applicaties												
	Onderdeel ->	K2Burgerzaken	GWS	MVV	Corsa	K2Datadistributie	K2Financiën	GisVG	imPROMPTU	Architectuur, werkplekken	K2Onderwijs	BAG	K2Begraven
Kwaliteit top-10	100	13	13	13	13	12	8	8	8	4	3	3	1
1. Koppelbaarheid (S)	21	XX	X	XXX	XXX	X	XX	X				XXX	
2. Beschikbaarheid (S)	19	X	X		XX		X	X					
3. Performance (S)	18	X			X								
4. Herstelbaarheid (S)	13												
5. Foutbestendigheid (S)	10		X	X	X			X					
6. Volledigheid (P)	8	X					X		X				
7. Degradeerbaarheid (S)	3	X			X								
8. Beheerbaarheid (S)	3	X		X					X	X	X		X
9. Klantgerichtheid (P)	3												
10. Doorlooptijd (P)	2						X						

Test dillema's:

- Risico is erg groot +++
- Test kost € 10.000
- Doen of niet doen?

- Risico is erg groot +++
- Test kost € 100.000
- Doen of niet doen?

- Risico is klein +
- Test kost € 10.000
- Doen of niet doen?

- Conclusie: alle keuzen zijn relatief.

Consequenties

- Moeilijk om nut van testen te bepalen,
  en zeker om het aan “leken” duidelijk te maken
- Kosten van een test hebben geen invloed op testplan
- Kunstmatige entry- en exit criteria
  in relatie tot opbrengst en kosten

- Daardoor geen “contact” met [project] management
  of Business Sponsors

Inhoudsopgave

1. ISACA
2. RISK IT
   - Doel
   - Structuur
3. RISK Appetite
   - Aanvulling op Risk Based Testen
4. Vragen

De oplossing: Langszij komen met Business

- Invloed van de Risk Appetite van de onderneming.
- Risico is tevens Kans

  ISACA's definitie van risico:

  Risk is a natural part of the business landscape.
  If left unmanaged, the uncertainty can spread like weeds.
  If managed effectively, losses can be avoided and benefits obtained.

Risk map

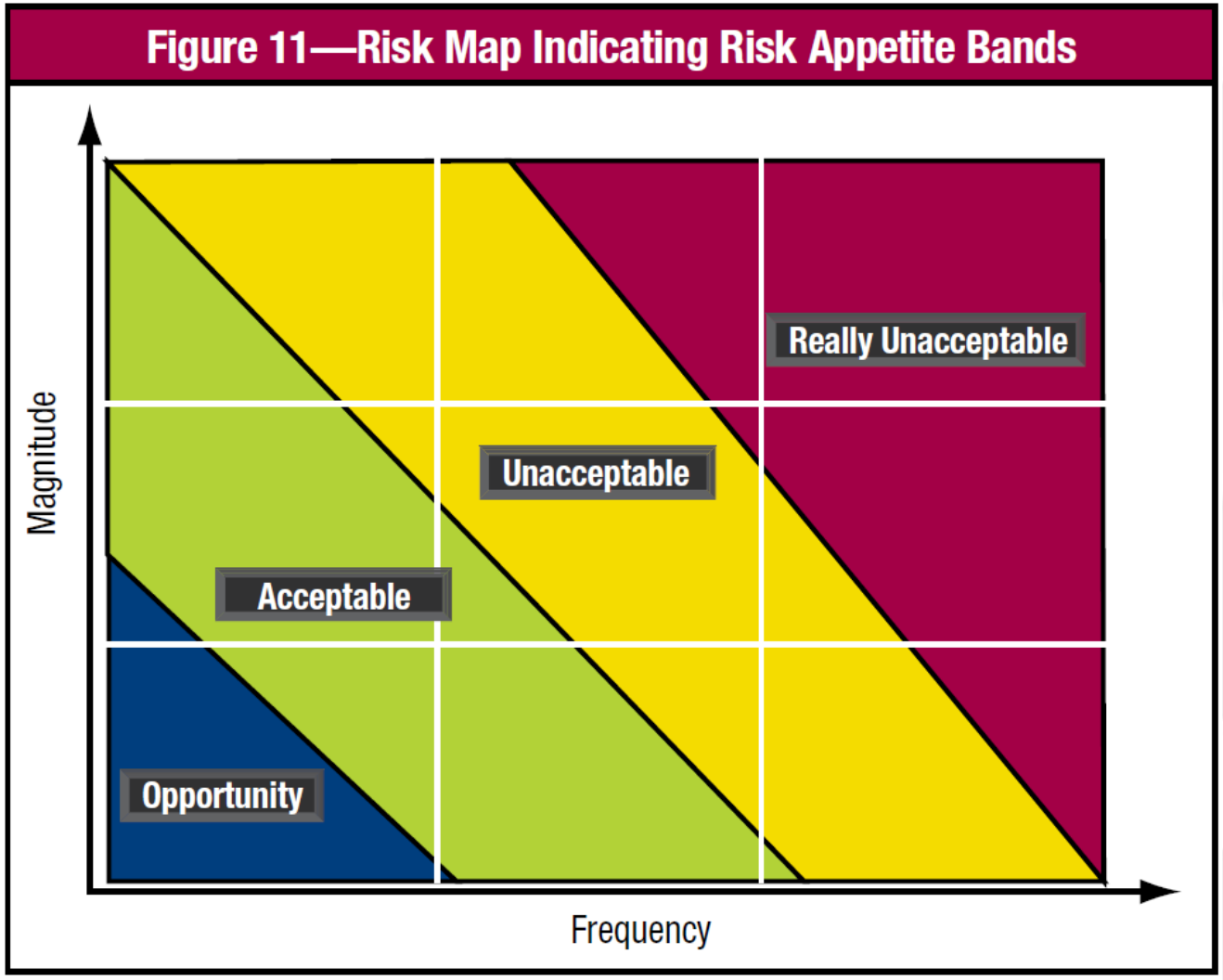
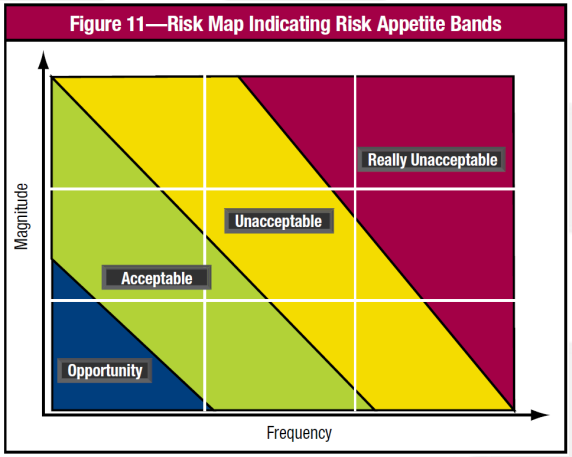


Figure 11—Risk Map Indicating Risk Appetite Bands
Really Unacceptable
Unacceptable
Acceptable
Opportunity
Magnitude
Frequency

Gebruikelijke acties

- Opportunity: kosten verlagen,
  meer risico accepteren
- Acceptable: geen maatregelen nemen,
  eventuele verliezen nemen
- Unacceptable: verzekeren, samenwerken,
  maatregelen nemen om naar acceptable te komen.
- Really unacceptable: vermijden, uitstappen,
  naar alternatieven zoeken



Hoe kennen we Risk Appetite?

Het gaat niet om de risico's, het gaat om hoe het bedrijf met wat voor soort risico's omgaat.

- Vragen naar beleidstukken
- Interviews met hoger management
- Waarden en normen opvragen
- Risico paragraaf in projectbrief (Prince 2)
- Hoe handelde het bedrijf in vergelijkbare gevallen?
- Wat zou je eigen inschatting zijn?

- En aan de orde stellen in de Risico analyse sessie!

Risico ligt in gebied “opportunity”

- Test kost € 10.000
- Doen of niet doen?

- Kans om € 10.000 te besparen!

- De testmanager als inkoper

Risico ligt in gebied “acceptable”

Het management is van mening dat het risico (eventueel na reeds genomen maatregelen) genomen kan worden

- Test kost € 10.000. Doen of niet doen?

- Vraag beantwoorden: wat levert het op,
  - Beter voorbereid zijn op falen van IT
  - Testen van maatregelen bij optreden risico
  - Terugdringen van de kans door oorzaakanalyse

  - De testmanager als sparring partner

Risico is “unacceptable”

Het management is van mening dat het risico (zelfs na genomen maatregelen) niet genomen kan worden

- Voorbeeld: Maandomzet = € 1.000.000 .
  Risico: 50% kans op verlies van € 1.000.000
- Test kost € 10.000
- Doen of niet doen?

- Interessant: test moet meestal wel gedaan worden
  maar niet als de kosten de pan uitrijzen, dan alternatief vinden

- Nodig: een zorgvuldige afweging van kosten en baten

- De testmanager als consultant

Risico is “really unacceptable”

Het management is van mening dat het risico (zelfs na alle genomen maatregelen) te groot is en het project desnoods moet stoppen

- Test kost € 10.000
- Doen of niet doen?

- Maakt niet veel uit: test moet gedaan worden, tenzij het project stopt. Het bedrijf wil het risico absoluut niet lopen.
- De uitkomst van de test is kritisch en wordt met argusogen bekeken.

- De testmanager als waarzegger
  -> focus op onderkennen alle risico’s
  -> kosten mogen toenemen om zekerheid te krijgen

Risico is ?????

- Maandomzet = € 1.200.000
- Risico: 50% kans op verlies van € 100.000
- Test kost € 10.000

- Doen of niet doen?

Risico is ????

- Maandomzet = € 1.200.000
- Risico is 5% op verlies van € 1.000.000
- Test kost € 10.000
- Doen of niet doen?

- En wat als de test 1 maand duurt en de verwachte opbrengst nog steeds € 1.200.000 per jaar is ??

Model maken

			Wel testen		Niet testen
			bedrag in €		bedrag in €
Testinspanning			€ -7.000		€ -
Testomgeving			€ -2.000		€ -
Overhead			€ -1.000		€ -
Gemiste opbrenst			€ -25.000		
Totaal kosten			€ -10.000		€ -
Herstelkosten			€ -1.250		€ -15.000
Blootgesteld risico	€	50.000			€ -50.000
Netto rendement van test			€ -36.250		€ -65.000
Böhm-factor		12			
Testduur in maanden		1			
Verwachte opbrengst per maand	€	25.000			
Kans op risico		5%			
Omvang risico	€	1.000.000			
Herstelkosten bij optreden risico	€	25.000			

Samenvatting

- Risk Appetite stuurt de testaanpak
- Verschillende soorten risico's vragen om verschillende benadering
- Kosten-Baten analyse geeft inzicht in welke test[soort]en zin hebben
- De (nog steeds absoluut noodzakelijke) risico analyse kan beperkt blijven tot te testen risico's
- Omdat testen beter aansluiten bij de Risk Appetite is de communicatie met de stakeholders optimaal
- De opbrengst van testen kan duidelijk gemaakt worden.

Vragen