Informatierisico's en –beveiliging:

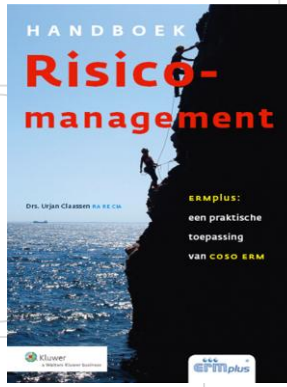
Een integrale benadering van beheersing (ERMplus)

Drs Urjan Claassen RA RE CIA
Vennoot Clascon

Urjan Claassen

Opleiding
Drs: Bedrijseconomie Tilburg
RA: Universiteit van Tilburg
RE: Erasmus Universiteit Rotterdam

Loopbaan
96-97 Philips Electronics
97-01 Andersen Accountants
01-05 KPMG IT Advisory
05- Clascon Risicomanagement



ISBN: 978 90 13 0640

Universitaire Docent
03-heden Business Universiteit Nyenrode, docent Advanced & Financial Auditing
04-heden Erasmus Universiteit Rotterdam, gastcolleges ICT Auditing en Risicomanagement
04 - 08 Universiteit Maastricht, docent Management Control en Interne Beheersing

Nevenfuncties
10-heden International Federation of Accountants (New York - USA) – Advisory councel risk management & internal controls – committee accountants in business
09-heden Hogeschool Arnhem Nijmegen, Raad van Advies post HBO opleiding Audit & Risicomgmt

Publicaties
2010 – Het hoe en waarom van risicomanagement – Controllersmagazine
2009 – Handboek risicomanagement, een praktische toepassing van COSO ERM – Kluwer
2007 – Van Sociale Zekerheid naar Sociale Assurance – Reed Elsevier
2006 – Handreiking samenwerking RA RE – NOREA

Contact

Email claassen.urjan@clascon.nl
Kantoor 040 – 22 31 030
Mobiel 06 - 22 32 20 42

Waar gaan we het over hebben?

- Inleiding informatierisico's
- Strategische en operationele risico's
- Hoe houden we ze beheerst?
- Integraal In Control Framework

Inleiding Informatierisico's

Hacking is greater threat than military attack

Source ZDNet UK, 30 Mar 2

Foreign warns t life is a hack at

The for on Thu comput bigger military

Site Rabobank gekraakt

Bankieren via Internet is niet veilig

Door een onzer redacteuren

ROTTERDAM, 20 MEI. Bankieren via Internet is niet veilig. Dat blijkt uit een publicatie in het blad *Computer Idee*. Redacteuren van het

an klanten van kgegevens et opzetten

n aan acteur M. Internet moet je

hoe het de Rabobank te

'Internetsites zijn zo lek als een mandje'

ANP

AMSTERDAM

Tientallen internetsites die web-software van Microsoft gebruiken, zijn zo lek als een mandje. Dat blijkt uit een onderzoek van de *Automatisering Gids*, waarvan de eigen site ook lek bleek.

Door het intikken van een 'opgerekte URL', zeg maar de naam van de internetsite met aanvullende standaardcommando's, kwam de broncode op het scherm. Zo kon onder meer de site van Ohra, Wehkamp, Primafoon, Free Record Shop en PinkRoccade worden gekraakt. Bij Wehkamp was het zelfs mogelijk wachtwoorden te achterhalen.

Volgens Wehkamps marketingdirecteur M. Laseur zijn de *hackers* niet verder gekomen dan een eerste laag. 'Ze hebben wat kun-

Twijfels over beveiliging

Stadsdeel Centrum mogelijk slachtoffer cybercriminaliteit

Van onze verslaggever

Amsterdam, 3 november – Bij de gemeente Amsterdam zijn waarschijnlijk tientallen uit gevoelige documenten ontvreemd. Vorige we circuleerden vertrouwelijke gegevens over burgers in verschillende nieuwsgroepen op internet.

oordvoerder van de gemeente erzoek en kunnen op dit mome ngen worden gedaan.

is of het incident het gevolg is veiligingsmaatregelen of nalati edewerkers. Volgens deskund ing bij veel organisaties te w

Hackers frustreren ook Nasdaq

WALL STREET

Van een onzer verslaggevers

New York - De plotselinge *hac*-gers rage in de Verenigde Staten egt niet alleen tal van vooraan-staande websites lam, maar frus-reert ook de aandelen van inter-netfondsen. Bijgevolg moest de Nasdaq-composite, die veel van dit soort fondsen herbergt, de winst die het gaandeweg de han-delsdag opbouwde uit handen ge-ven. Voor het eerst deze week ein-digde de Nasdaq in de min: 63,56 punten en nu op 4161 punten. Ook de toonaangevende Dow Jo-nes-index ging gisteren onderuit (-35 procent) en eindigde net on-der de 10.700 punten.

Beleggers reageerden ge-schrokken op het hackersgeweld en concludeerden dat het internet wellicht toch een wat minder soli-de investering is dan ze dachten. Getroffen fondsen zijn onder meer E*Trade (min $ 1.12 op $ 21.88), virtuele boekwinkel Amazon.com (bijna $ 3 eraf op een dikke $ 80) en de maandag gecrashte zoekmachine Yahoo! (liefst $ 10,50 verlies' op $ 362,62). Zelfs Cisco Systems, dat dinsdag nabeurs nog zulke uitstekende kwartaalcijfers pre-senteerde, voelde nattigheid. De fabrikant van noodzakelijke in-ternetapparatuur zag zijn aan-deel aanvankelijk met ruim $ 6 omhoog spuiten, maar moest zich bij de slotgong tevreden stel-len met een winst van $ 3, net on-der de $ 129.

Maar zoals bekend is de één zijn dood de ander zijn brood. En dus lachten bedrijven die het in-ternet tegen hackers en ander ge-spuis beschermen in hun vuistje. Fondsen met veelzeggende na-men als Watchguard Tec ($ 15,5 erbij op ruim $ 49), SonicWall Inc. (plus $ 10,5 op $ 72,75) en Ve-riSign (een royale $ 5 winst) tra-den even uit de anonimiteit. Er was ook nog 'normaal' bedrijfs-nieuws. Zo presenteerde fris-drankengigant PepsiCo. fraaie winstcijfers over de laatste drie maanden van 1999: $ 490 mil-joen of 33 dollarcent per aandeel. Dat was 37 procent hoger dan een jaar eerder en bovenin de ver-wachtingen-*range* van analisten. Als beloning mocht het Pepsi-aandeel $ 0,69 omhoog naar $ 34 rond. En Microsoft hoorde onge-twijfeld tot zijn ongenoegen dat de Europese Concurrentiecom-missaris Monti een onderzoek is begonnen naar mogelijk mis-bruik van de toch al dominante positie van de Amerikaanse soft-warereus. Het bedrijf van Bill Gates en Steve Ballmer moest zo'n 5 procent van zijn beurs-waarde prijsgeven en staat nu op $ 104.

On-Line Intruder Steals 300,000 Credit Card Files

Valid Account Numbers Are Posted on the Net

By John Markoff
New York Times Service

SAN FRANCISCO — A mysterious computer intruder tried to extort $100,000 from an Internet music retailer after claiming to have copied its collection of more than 300,000 customer credit-card files, which could be used by others to charge purchases on-line or by telephone.

chief technology officer of SecurityFocus.com, a computer security firm. On Friday, Mr. Levy's company began alerting journalists to the existence of a World Wide Web site that the blackmailer had been using for two weeks to distribute perhaps 25,000 stolen card numbers to thousands of other people. That site was shut down early Sunday morning.

"On the Internet you can have crimi-nals coming from countries where we radium treaties," Mr. Levy w do you prosecute these eveq investigate their

erse is an on-line music store eUniverse Inc., of Walling-necticut. An eUniverse ex-d that the company had been with the FBI in an effort to extortionist. "He definitely niverse data," said the ex ad Greenspan. "Whether he site or got the data in some I'm not sure exactly."

anspan said the company had ing e-mail notices to its cus-rting them to the theft, and

EXTORT, Page 4

k in website Univé, gevens op straat

en onzer redacteuren

TERDAM, 31 JAN. Door een lek in de website erzekeringsmaatschappij Univé zijn afgelopen einde persoonlijke gegevens van klanten baar geworden. De site is gekraakt door de landse hackersgroep HIT2000 (Hacking Into

en lek in de computerprogramma's die Univé de website gebruikt, zijn gegevens bekend rden van klanten over het soort verzekeringen hebben lopen bij Univé. Ook namen, sen en polisnummers van klanten zijn baar geworden. Het betreft gegevens die n via de website van Univé hebben ingevuld. In sommige gevallen is precies te zien welke verzekeringen een klant bij Univé heeft afgesloten, hoe de financiële situatie is en wat de gezinssituatie is.

Vertrouwen in ASP geschaad

Computable 1-9-2000

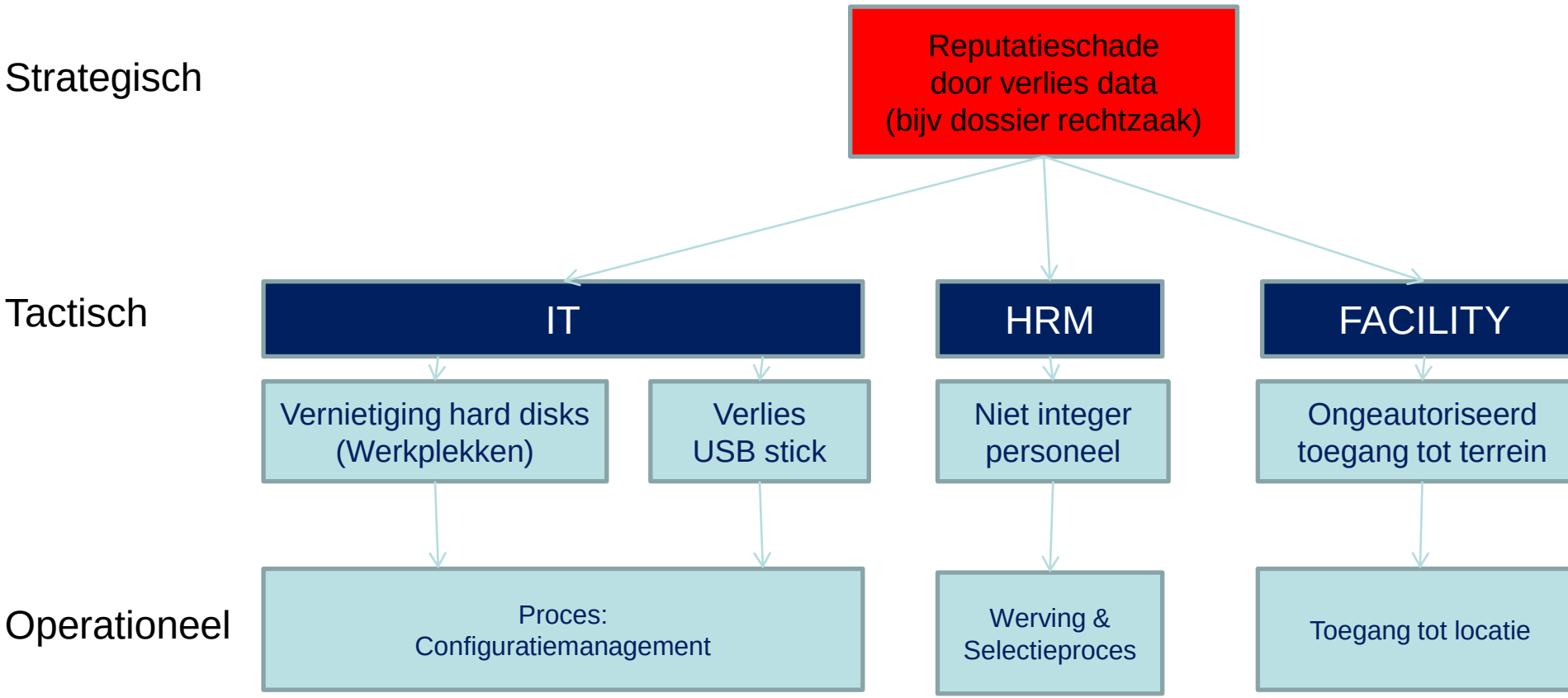
Slechte gegevensbescherming bij Annapa brengt schade toe aan het vertrouwen in het ASP-model, meent Sander van Haaff.

Een aantal weken geleden is Annapa.com gelanceerd, een nieuw soort website die administratieve functionaliteiten via het Web aanbiedt. Zo kun je er je afspraken bijhouden en zaken als telefoonnotities bewaren. Hoewel de toegevoegde waarde van de geboden functionaliteit mijns inziens beperkt is (er zijn immers al zoveel gratis 'lokale' equivalenten), is vooral de achterliggende gedachte bij deze site van enorm belang. Het betreft het veelbelovende ASP-model (*application service provider*) waarover de laatste tijd zoveel wordt geschreven. Wanneer je naar Annapa surft, ontmoet je een voorzichtig glimlachende dame op leeftijd die onder meer vertelt dat 'privacy enorm belangrijk is' en dat 'Arthur Andersen Annapa controleert om uw privacy te waarborgen.' Aangezien we bij ons bedrijf hard bezig zijn uitgebreide ASP-applicaties te ontwikkelen, is mijn belangstelling gewekt. En dus keek ik in hoeverre uw (en mijn) privacy daadwerkelijk wordt beschermd bij Annapa. Ik viel haast van verbazing van mijn stoel toen ik ontdekte hoe kinderachtig makkelijk het is om informatie in te zien van andere gebruikers, en deze te wijzigen. Een simpele aanpassing in de URL is voldoende.

Hoewel ik het jammer zou vinden als Annapa op een mislukking zou uitlopen, is het uiteraard geheel aan de makers (en partners) van Annapa om te bepalen in welke mate Annapa beveiligd moet zijn. Wat mij echter wel aan het hart gaat – mede vanwege het feit dat ons bedrijf in dezelfde markt opereert – is dat Annapa naar mijn mening grote schade toebrengt of kan toebrengen aan het vertrouwen van gebruikers van het ASP-model (c.q. de applicaties die volgens dit model worden aangeboden). Persoonlijk wil ik mijn agenda niet delen met derden en mijn administratie al helemaal niet. Uiteraard ben ik er niet op uit om Annapa enige schade te berokkenen, maar omdat ze niet op hun eigen feedback-optie reageren, probeer ik via dit forum (*Computable Online*, red.) de bouwers nogmaals te overtuigen van de problematiek rond Annapa.

Sander van Haaff, internet technology consultant

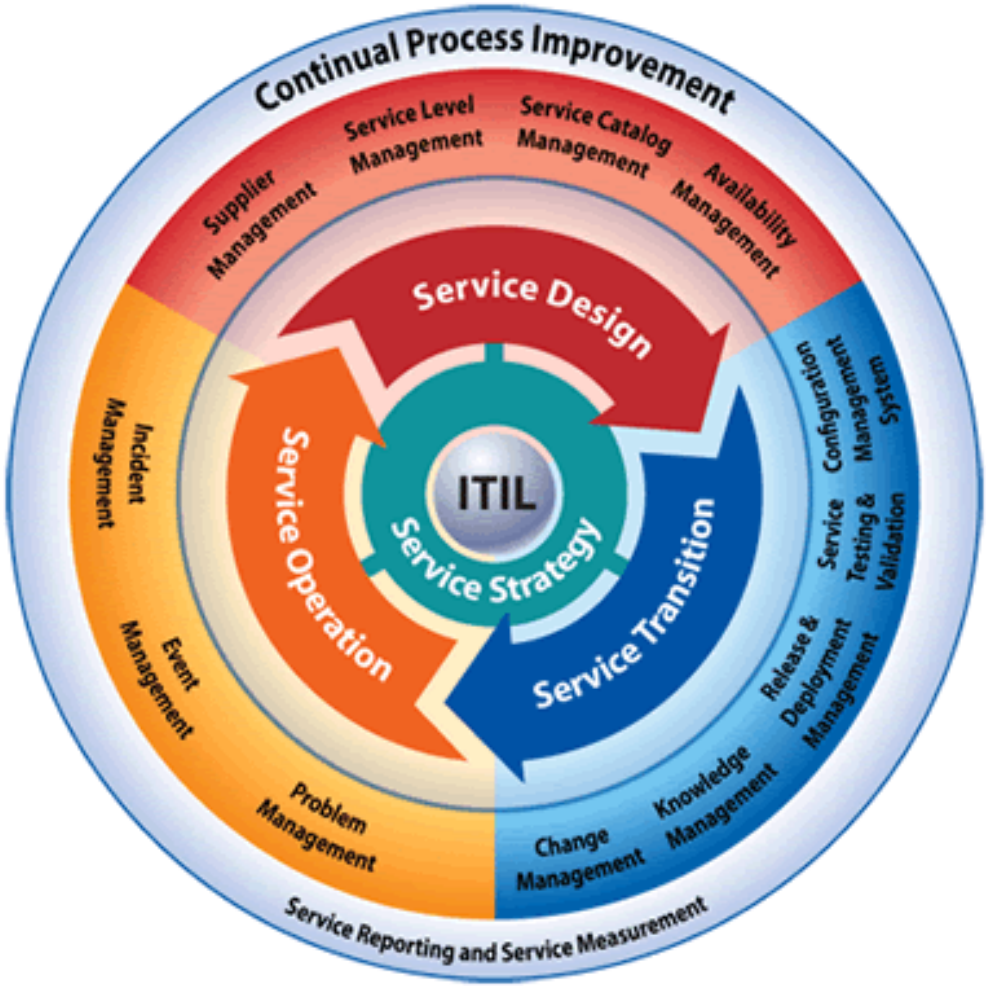
Strategische en operationele risico's



Code voor Informatiebeveilig

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmiddelen
4. Beveiligingseisen voor personeel
5. Fysieke beveiliging
6. Beheer communicatie en bedieningsprocessen
7. Toegangsbeveiliging
8. Ontwikkeling en onderhoud van systemen
9. Continuiteitsmanagement
10. Naleving

Waar lopen we tegen aan?.... **IT**



IT Organisatie

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmi
4. Beveiligingseisen voor personeel
5. Fysieke beveiliging
6. Beheer communicatie en bedieningsp
7. Toegangsbeveiliging
8. Ontwikkeling en onderhoud van syste
9. Continuiteitsmanagement
10. Naleving

Waar lopen we tegen aan?....**HRM**

HRM afdeling

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Beveiligingseisen voor persone
4. Beheer communicatie en bedie
5. Toegangsbeveiliging
6. Naleving

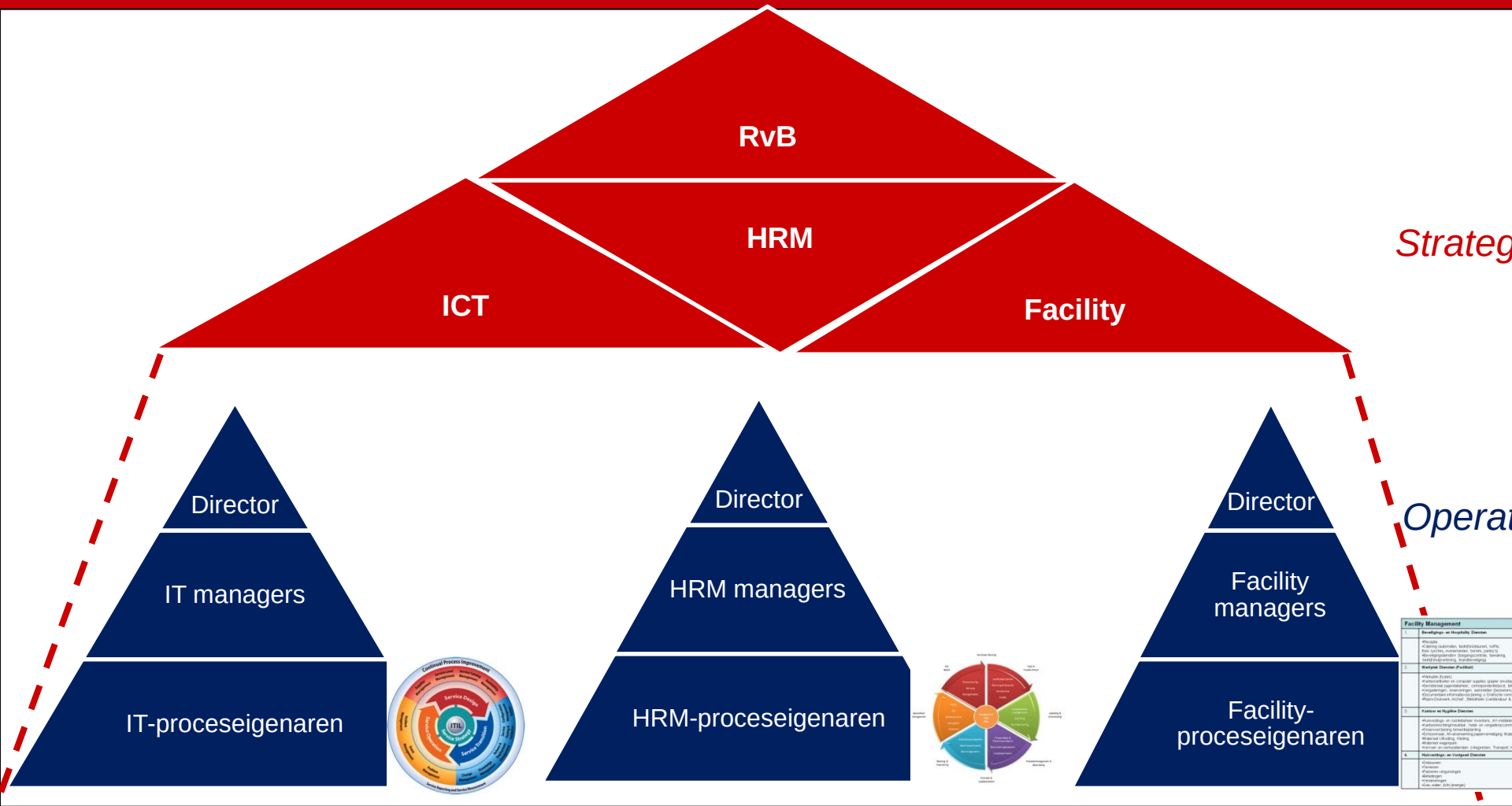
Waar lopen we tegen aan?....**FACILITY**

Facility Management	
1.	**Beveiligings- en Hospitality Diensten**
	•Receptie •Catering (automaten, bedrijfsrestaurant, koffie, thee, lunches, evenementen, borrels, pantry's) •Beveiligingsdiensten (toegangscontrole, bewaking, bedrijfshulpverlening, brandbeveiliging)
2.	**Werkplek Diensten (Facilitair)**
	•Werkplek (fysiek) •Kantoorartikelen en computer supplies (papier enveloppen) •Secretariaat (agendabeheer, correspondentie/post, telefoon, •Vergaderingen, reserveringen, aanmelden (bezoekers, toegangsID) •Documentaire informatievoorziening o Grafische vormgeving/ (DTP), Postkamer, •Repro-Drukwerk, Archief , Bibliotheek (vakliteratuur & abonnementen)
3.	**Kantoor en Hygiëne Diensten**
	•Huisvestings- en ruimtebeheer inventaris, AV-middelen •Kantoorinrichting/meubilair, hotel- en vergaderaccommodatie •Groenvoorziening binnenbeplanting •Schoonmaak, Afvalverwerking papiervernietiging Materiaal- en Materieel Diensten •Materiaal Uitrusting, Kleding •Materieel wagenpark •Vervoer- en verhuisdiensten (vlieg)reizen, Transport, Koerier, Mailing
4.	**Huisvestings- en Vastgoed Diensten**
	•Gebouwen •Terreinen •Parkeren vergunningen •Belastingen •Verzekeringen •Gas, water, licht (energie)

Facility Management

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsm
4. Beveiligingseisen voor personeel
5. Fysieke beveiliging
6. Beheer communicatie en bedienings
7. Toegangsbeveiliging
8. Naleving

Op strategisch en operationeel niveau

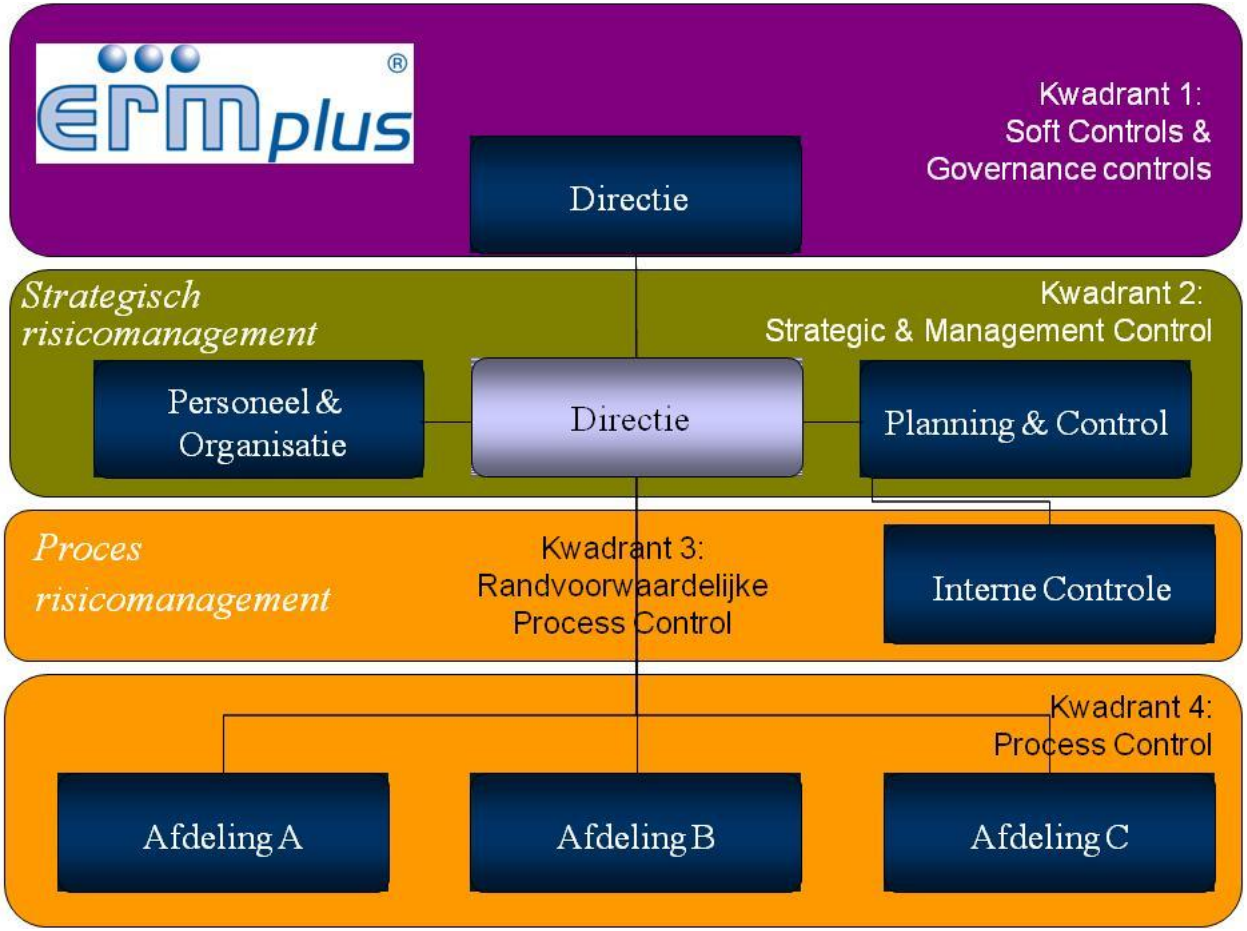


Lines of Defense

VERDEDIGINGSLINIES VOOR RISICOMANAGEMENT

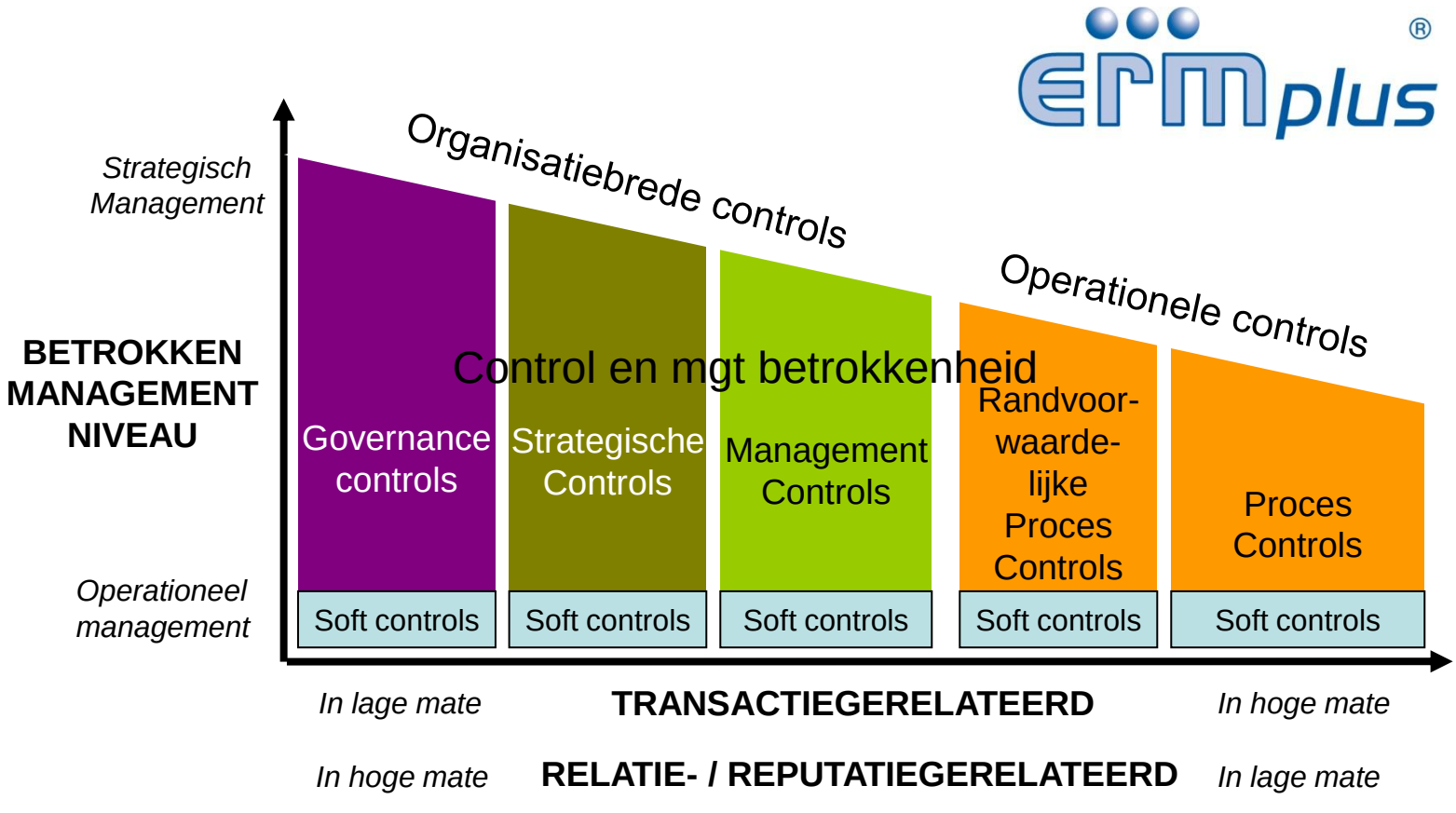
- Maar hoe waarborgen we de samenhang?

ERMplus (1)



www.ermplus

ERMplus (2)

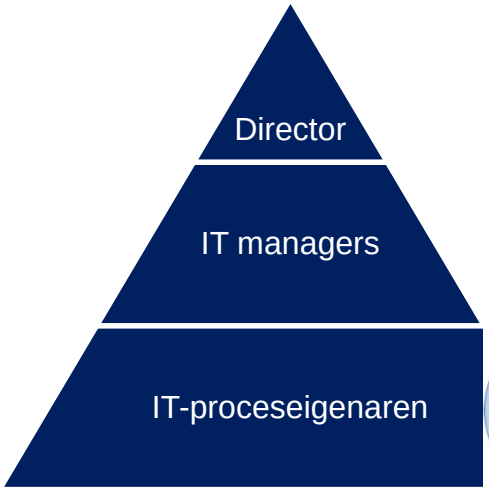


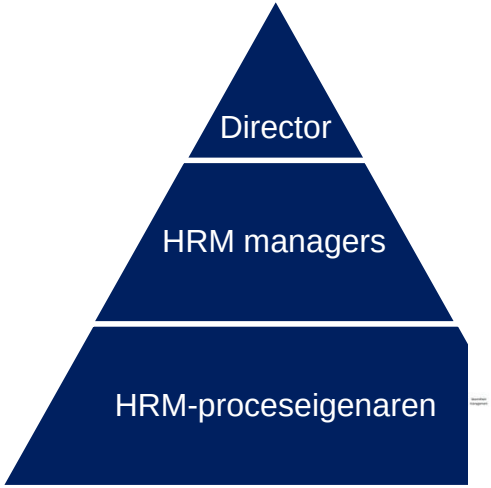
www.ermpl

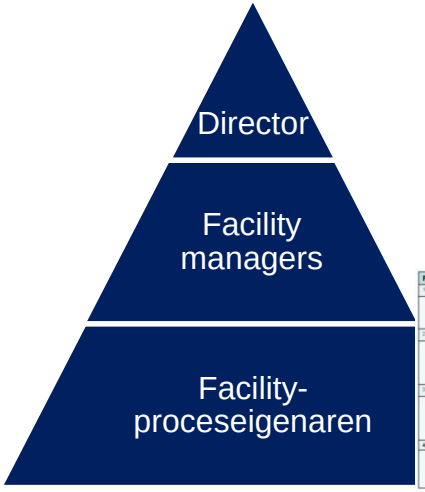
ERMplus (3)

Kwadrant	Omschrijving	Type Interne beheersingsmaatregelen
Kwadrant 1	Soft Controls	- Zachte beheersingsmaatregelen die de overige kwadranten versterken of verzwakken - Normen: COSO ERM, Quinn & Cameron e.d.
Kwadrant 2	Interne management beheersing	**Strategische planning:** -Beleidsvorming & Rapportage
		Management Control: - Organisatiestructuur - Inrichting bedrijfsprocessen - Resultaatgebieden managers - budgettering - Beoordeling en belonen
		Taakbeheersing: - Management toezicht o.b.v. rapportages uit de lijn - Stuurgroep en programmamanagement - KPI's en benchmarking - Auditrapportage
Kwadrant 3	Randvoorwaarde procescontroles	**Functiescheidingen:** - Binnen AO-beschrijvingen - Competentietabellen binnen applicaties
		Algemene ICT controles: - Change management - Continuiteitsmanagement - Beheer en onderhoud
Kwadrant 4	Procescontroles	- Handmatige controles - Applicatiecontroles

Control in samenhang





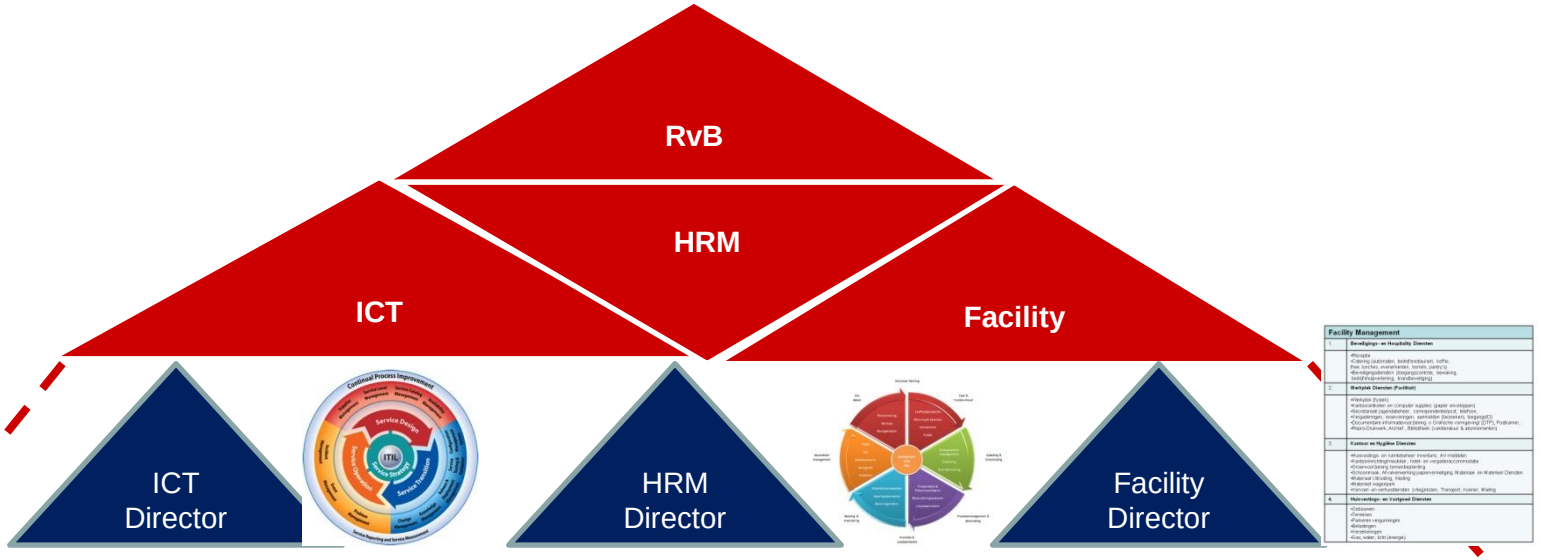


Tactisch

Operationeel

Mgmt Controls	Task Controls		Randvoor-waarde-lijke Proces Controls	Proces Controls
Soft controls	Soft controls		Soft controls	Soft controls

Control in samenhang



Strategisch

Tactisch

Governance controls	Strategic Controls	Mgmt Controls	Task Controls		Mgmt Controls	Task Controls
Soft controls	Soft controls	Soft controls	Soft controls		Soft controls	Soft controls

Vragen?

- Meer informatie: www.ermplus.nl

- **Bedankt voor uw aandacht!**

Clascon, hét adviesbureau voor risicomanagement.

Clascon Audit & Consulting, De Neerheide 12D, 5581 TP Waalrre
T: 040 - 2231030, F: 040 – 2231039, E: info@clascon.nl, I: www.clascon.nl