IBP met Focus

saMBO-ICT 5-2-2016

Jaap de Mare, informatiemanager Albeda College

Albeda College

- Rotterdam en omstreken (ook ‘buitenlocaties’)
- 20.000 studenten
- 8 relatief zelfstandige branches
- innovatief t.a.v. de inzet van ICT

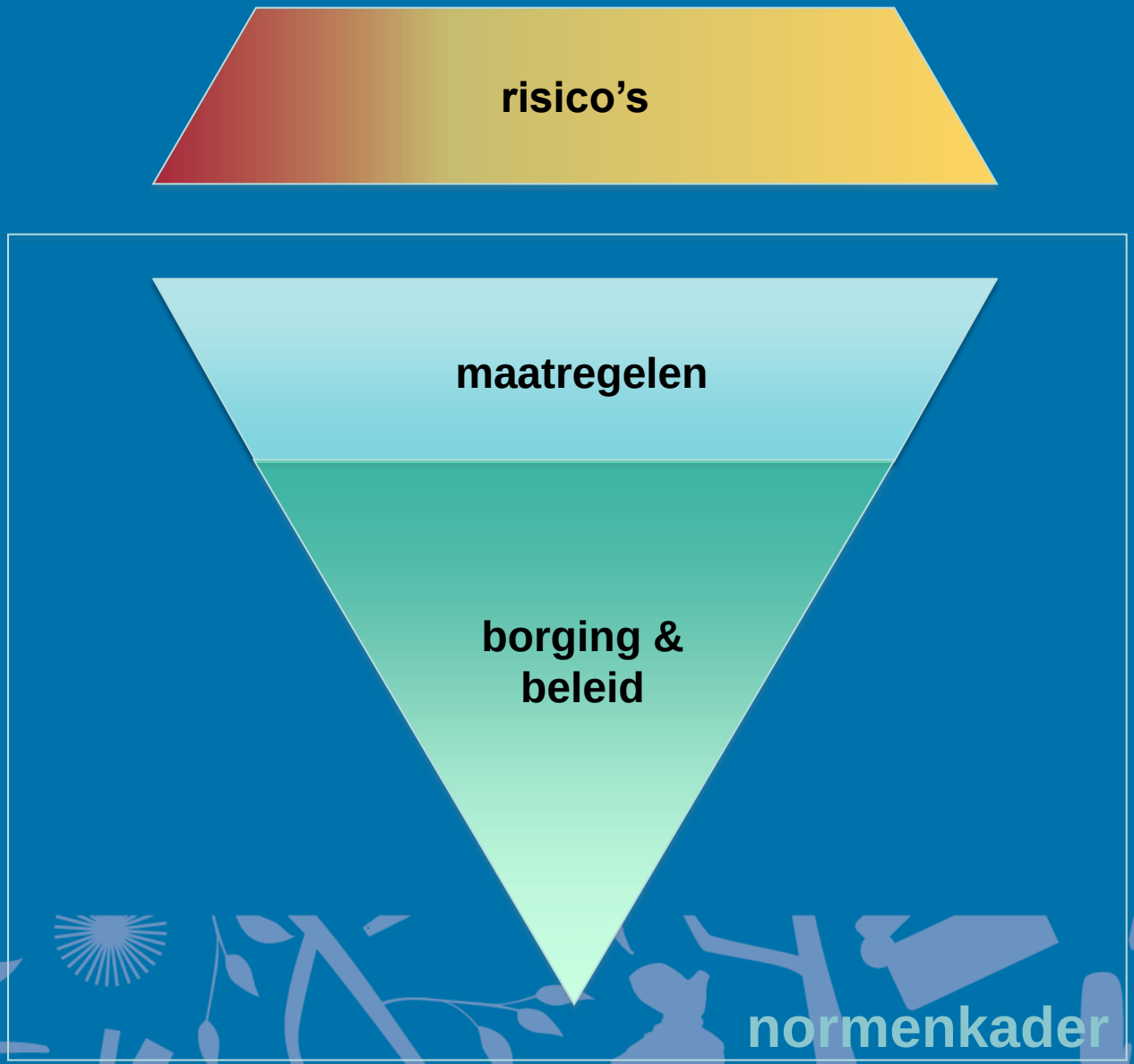
IBP bij Albeda - ontstaansgeschiedenis

- In 2013 gestart met IBP; benoeming Security Officer
- In 2014 IBP-beleid door CvB aangenomen, gebaseerd op Code Informatiebeveiliging Hoger Onderwijs
- Begin 2015 Security Officer deelname aan Masterclass
- Eind 2015 Informatiemanager deelname aan Masterclass
- IBP nu nog belegd bij ICT; discussie om het bij IM te beleggen

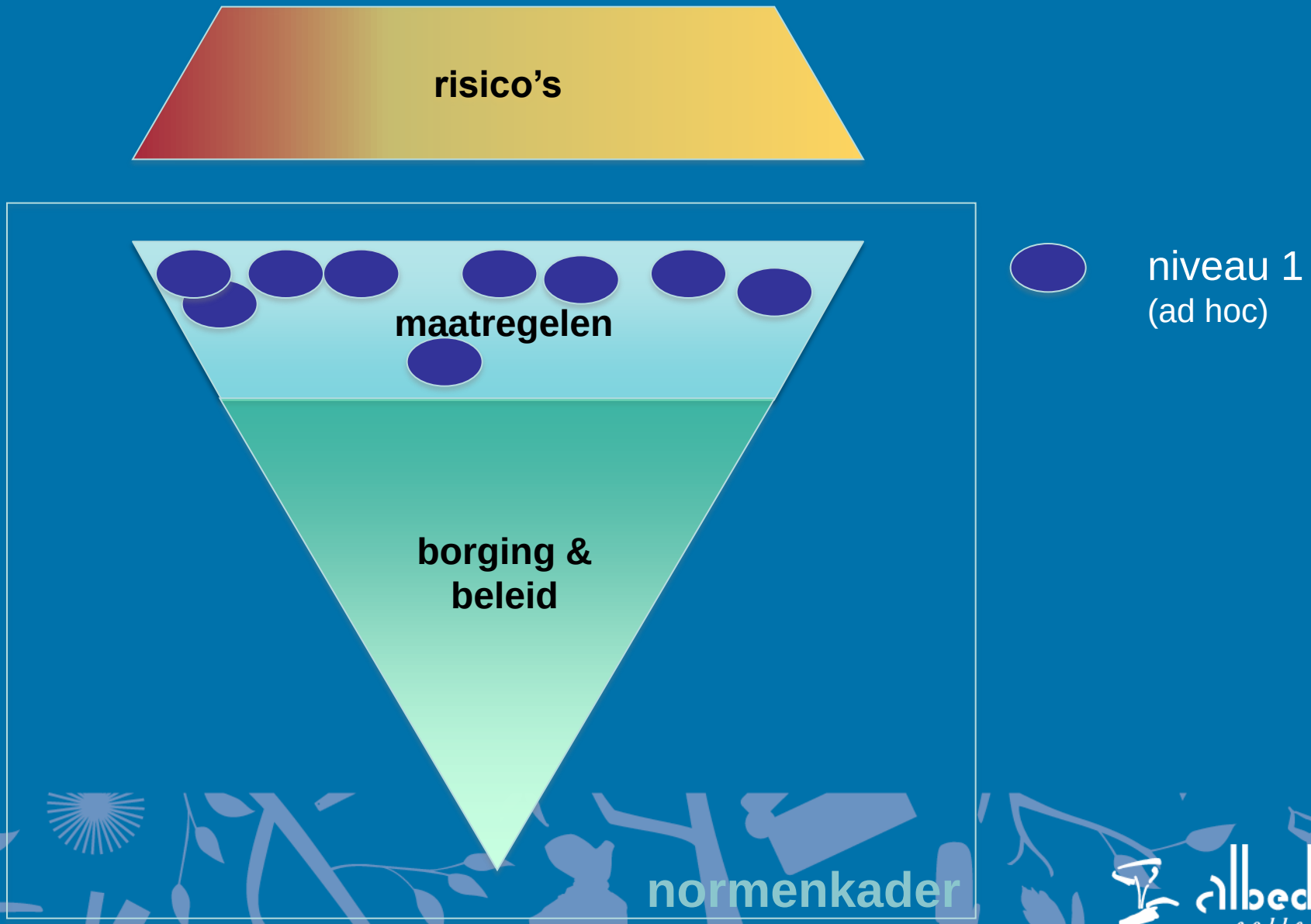
Stand van Zaken

- Inschatting score toetsingskader: ongeveer 2,0
- Veel activiteiten op het gebied van beleidsvorming:
  - outline voor ruim 40 beleidsstukken (‘richtlijnen’) geformuleerd
  - daaronder nog enkele tientallen andere beleidsstukken benoemd
  - inrichting Topdesk, identificeren Bedrijfskritische Applicaties
  - rol van Security Officer steeds beter uitgekristalliseerd; wordt steeds beter gevonden
  - governance nog niet goed belegd
- Beperkt zichtbare resultaten

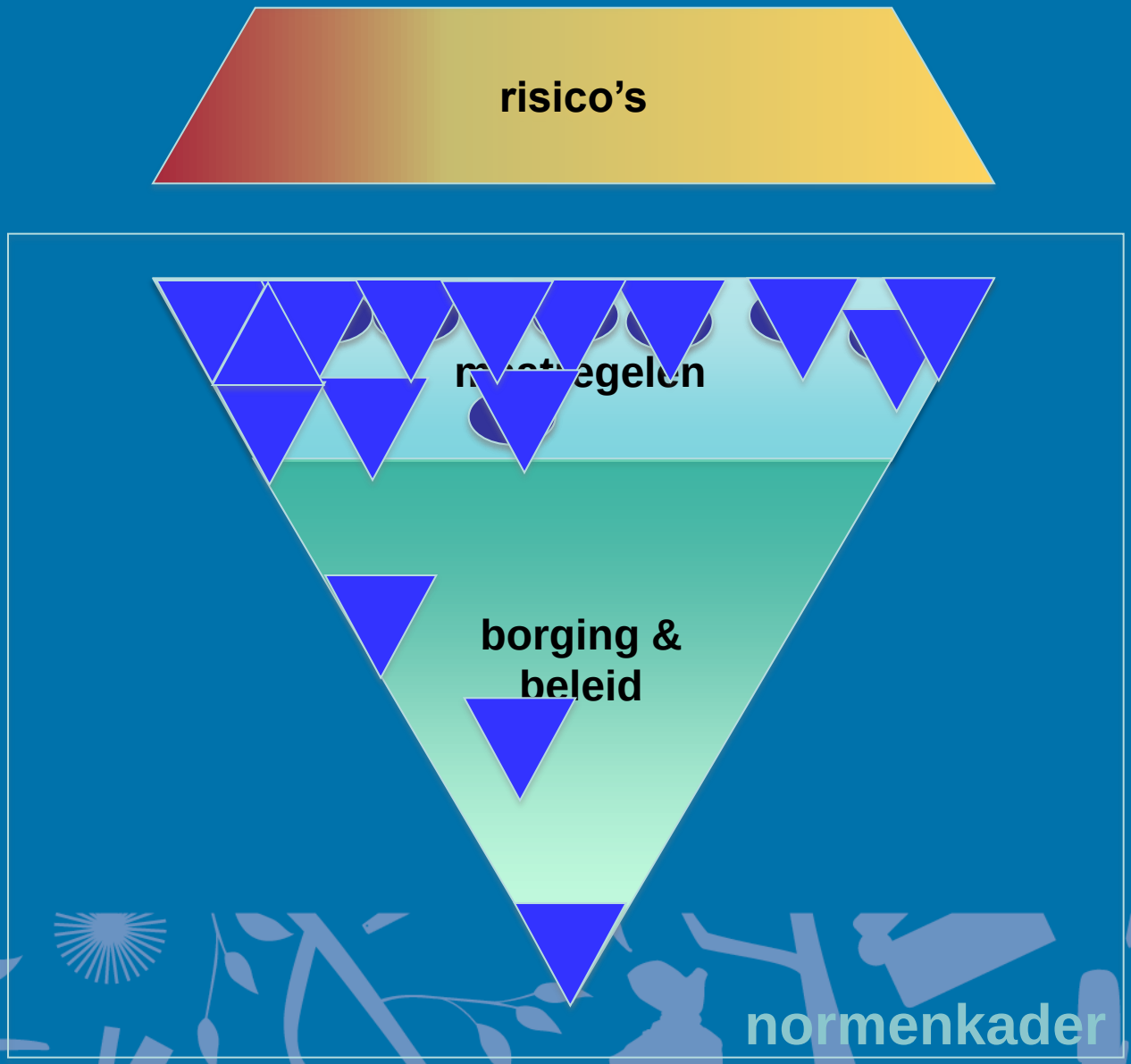
denkkader voor IBP



denkkader voor IBP



denkkader voor IBP

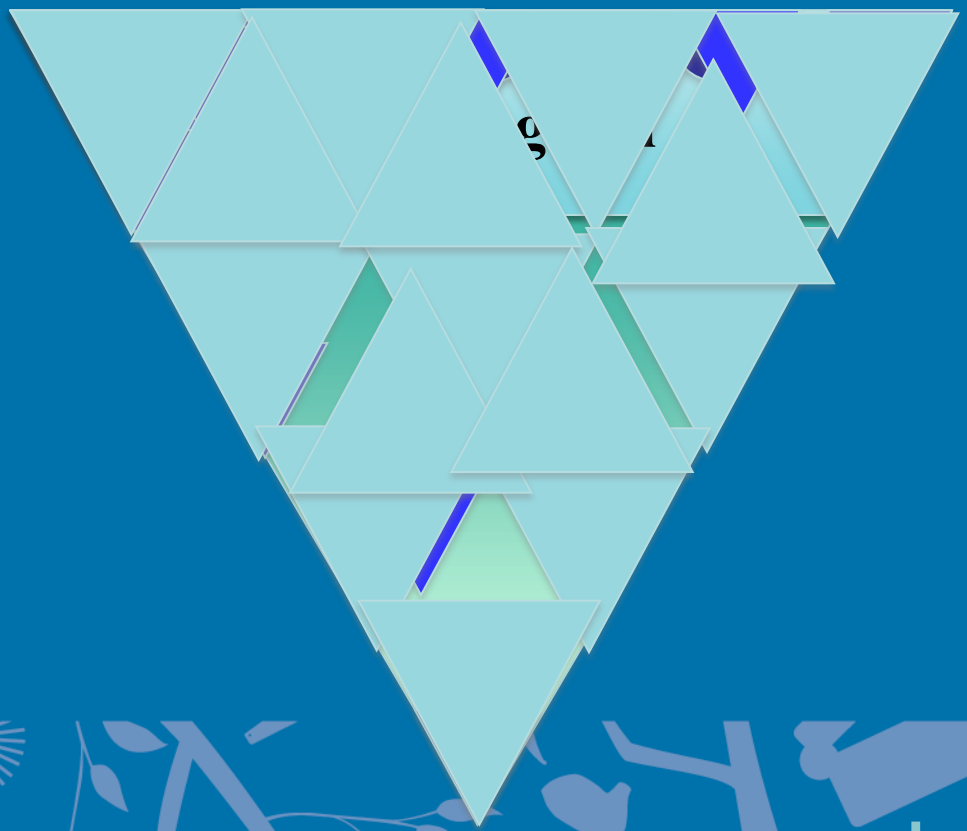


niveau 1
(ad hoc)

niveau 2
(herhaalbaar maar intuitief)

albeda college

denkkader voor IBP



niveau 1
(ad hoc)

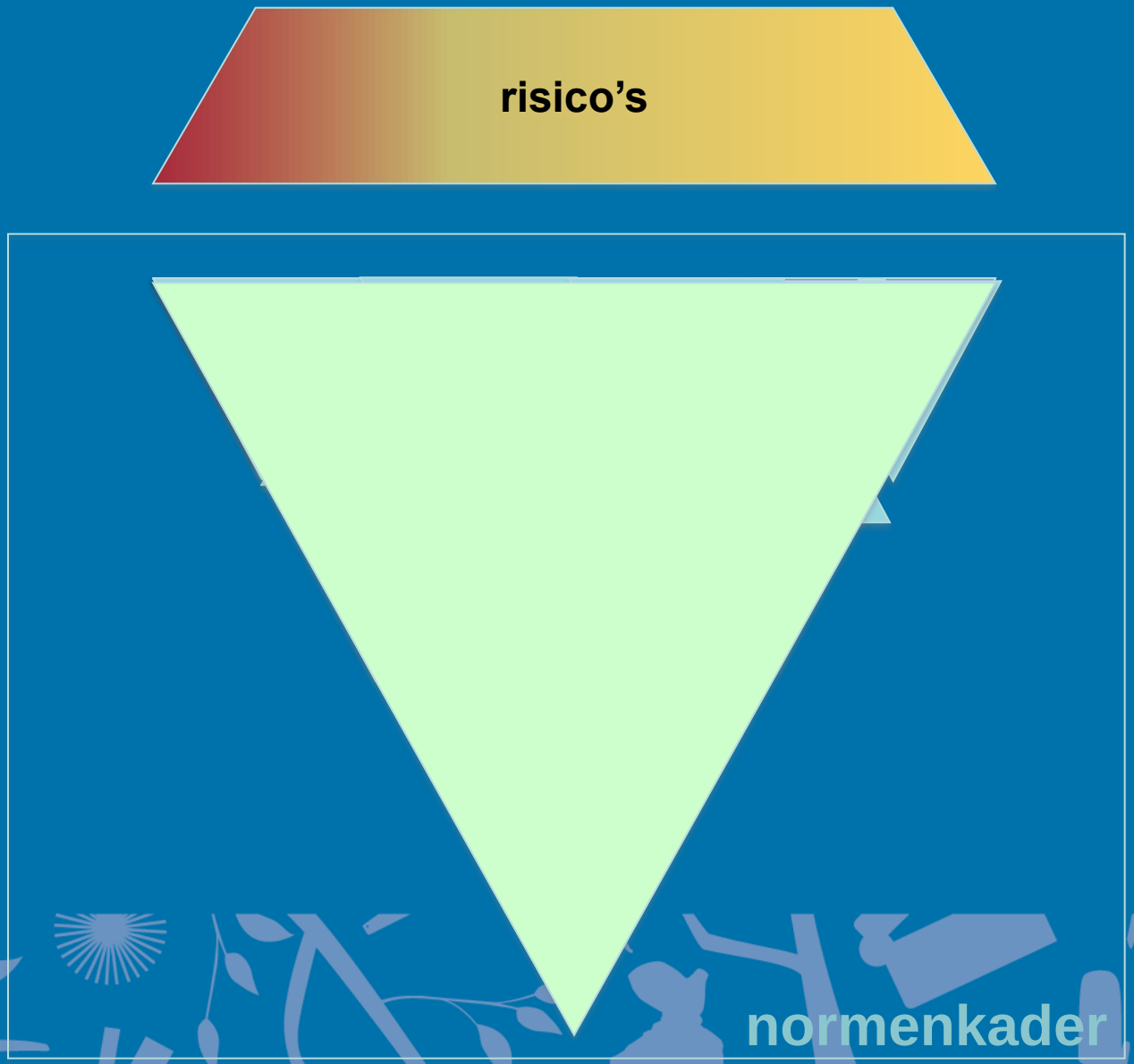
niveau 2
(herhaalbaar
maar intuitief)

niveau 3
(gedefinieerd
proces)

normenkader

albeda college

denkkader voor IBP



niveau 1
(ad hoc)

niveau 2
(herhaalbaar
maar intuitief)

niveau 3
(gedefinieerd
proces)

niveau 4
(beheerst en
meetbaar)

albeda college

Herijking IBP: Focus!

- Focus op grote en midden risico’s (op basis van Surf Cyber-dreigingsbeeld Hoger Onderwijs)
- Focus op maatregelen

Surf cyberdreigingsbeeld Hoger Onderwijs

OVERZICHT DREIGINGEN

Type Dreiging	Manifestatie van dreiging		Actoren	Voorbeeld Incidenten	Relevantie (kans x impact)		
Type Dreiging	Gebeurtenis				Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	• Onderzoeksgegevens worden gestolen • Privacygevoelige informatie wordt gelekt en gepubliceerd • Blauwdruk van opstelling onderzoeksinstellingen komt in verkeerde handen • Fraude door verkrijgen van data over toetsen en opgaven	→	• Cybercriminelen • Activisten • Staten • Medewerkers	• Tentamenfraude door openbaarmaking van tentamenopgaven • Privacygevoelige gegevens over studenten en leerlingen op straat beland • Kamervragen over intranetlek Hogeschool	MIDDEN	HOOG	MIDDEN
2.Identiteitsfraude	• Student laat iemand anders examen maken • Student doet zich voor als andere student of medewerker om inzage te krijgen in tentamens • Activist doet zich voor als onderzoeker • Student doet zich voor als medewerker en manipuleert studieresultaten	→	• Studenten • Cybercriminelen • Activisten	• Kamervragen naar identiteitsfraude Hogeschool Windesheim • Fraude in toelating examens	HOOG	MIDDEN	LAAG
3. Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata of examendata worden vernietigd • Opzet van onderzoeksinstellingen wordt gesaboteerd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	↑	• Cyberonderzoekers • Activisten • Studenten • Medewerkers	• Distributed Denial of Service aanval treft SETI project • Dorifelvirus treft ook universiteiten • Server legde netwerk Universiteit Utrecht plat	MIDDEN	MIDDEN	MIDDEN
4. Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Manipulatie van onderzoeksgegevens • Aanpassing van bedrijfsvoering data	↓	• Studenten • Medewerkers	• Student krijgt vier jaar celstraf voor het wijzigen van zijn cijfers • Massale fraude economiestudenten • Student hackt website en inleversysteem Informatica	HOOG	LAAG	LAAG
5. Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	→	• Staten • Bedrijven & commerciële partnerinstellingen • Cybercriminelen	• MI5 waarschuwde Britse universiteiten voor cyberaanvallen • NSA hackt Belgische cyberprofessor • Chinezen bespioneren denk tanks met expertise in Irak	LAAG	HOOG	LAAG
6. Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	→	• Cybercriminelen • Studenten • Medewerkers	• Yahoo blokkeert Universiteit Maastricht wegens spam • Student gebruikt universiteit computers om dogecoin te minen	LAAG	MIDDEN	MIDDEN
7. Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	→	• Activisten • Studenten • Cyberonderzoekers • Cybervandalen	• Homepage Faculteit Letteren beklad • Hackers bekladden website van MIT	LAAG	LAAG	LAAG

Impact van de dreiging t.o.v. 2014: ↓ = afgenomen, → = gelijk gebleven, ↑ = toegenomen

LAAG	MIDDEN	HOOG
"Er zijn geen nieuwe trends of fenomenen waar de dreiging van uitgaat. *OF* Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. *OF* Er deden zich geen noemenswaardige incidenten voorgedaan in de rapportageperiode."	"Er zijn nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat. *OF* Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. *OF* Incidenten deden zich voor buiten Nederland, enkele kleine in Nederland."	"Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken. *OF* Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. *OF* Incidenten deden zich voor in Nederland."

Legenda relevantie - *Bron: Cybersecuritybeeld Nederland (Nationaal Cyber Security Centrum, 2015)*

Informatie	Onderwijs	Onderzoek	Bedrijfsvoering
Studieresultaten	■		
Onderzoeksgegevens & Intellectueel eigendom		■	
CBRN+ gegevens		■	
Bedrijfsvoering data			■
Persoonsgegevens	■	■	■
Commercieel & Juridisch			■
Gegevens van (onderzoeks)partners		■	■
Gegevens over toetsen	■		

Hoge en midden dreigingen MBO

Hoog:

•Digitale identiteitsfraude (student geeft zich uit voor een ander tijdens digitaal examen)

•Manipulatie van digitaal opgeslagen data (student wijzigt cijfers in studentvolgsysteem)

Midden:

•Vertrouwelijke gegevens van studenten of medewerkers komen ‘op straat’ te liggen (b.v. zorggegevens, salarisbeslag)

•Diefstal examens (om te verkopen of voor eigen gebruik)

•Verstoring ICT (DDos aanvallen, phishing, spamming, virusaanvallen)

Hoge/midden dreigingen: maatregelen en borging

Maatregelen o.a.:

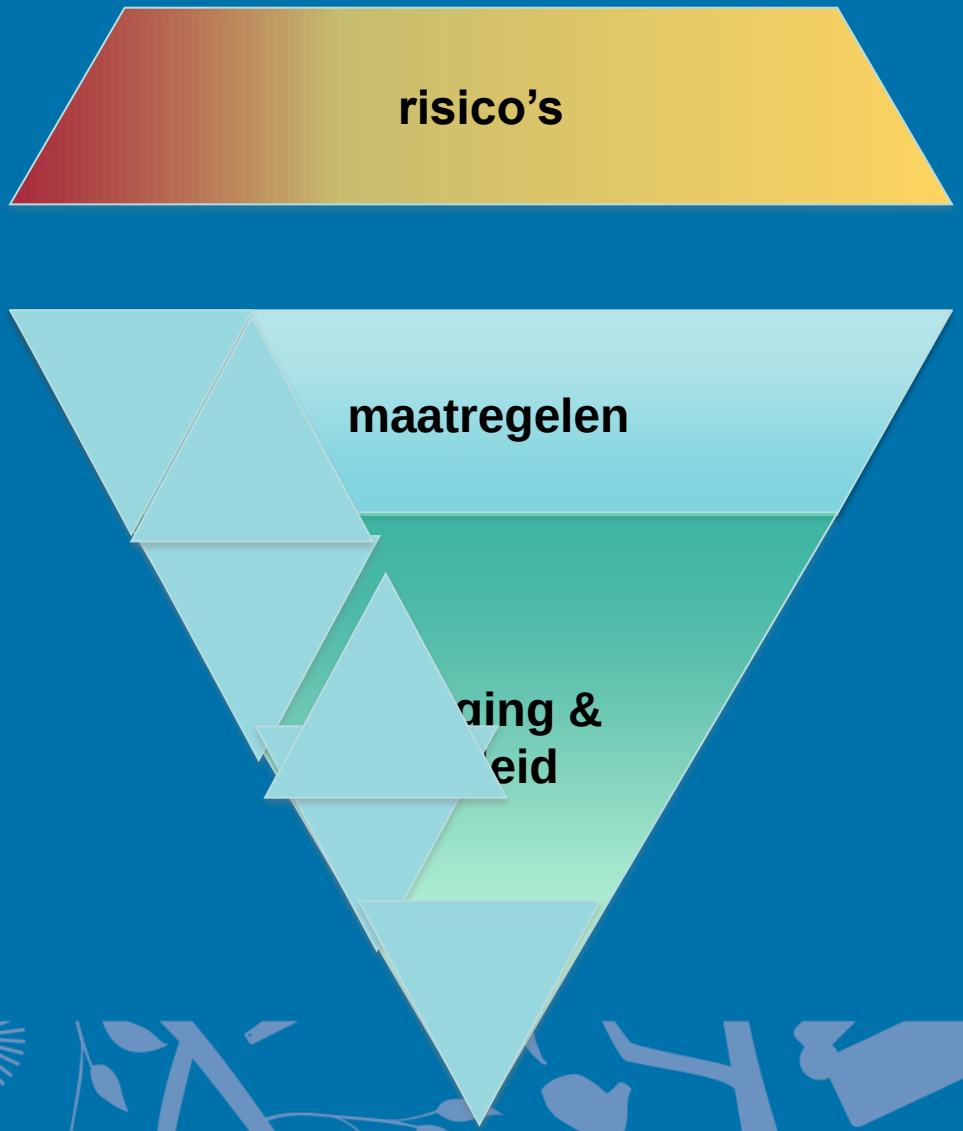
- sterke authenticatie bij ingeven cijfers (tokens)
- cijfers, en wijzigen van cijfers, monitoren
- versleutelen van bepaalde informatie (ook in koppelingen)
- geen ‘single sign on’ maar ‘simple sign on’
- bewustwordingscampagne bij medewerkers én studenten
- allerlei technische maatregelen tegen verstoringen

Borging o.a.:

- heldere procedures rond digitale examens
- heldere procedures rond opslag examens; monitoren
- back-up en restore borgen (o.a. oefenen)
- registreren en classificeren van beveiligingsincidenten

albeda college

geborgde aanpak hoge/midden risico's



niveau 3
(gedefinieerd proces)

Focus op maatregelen: laaghangend fruit

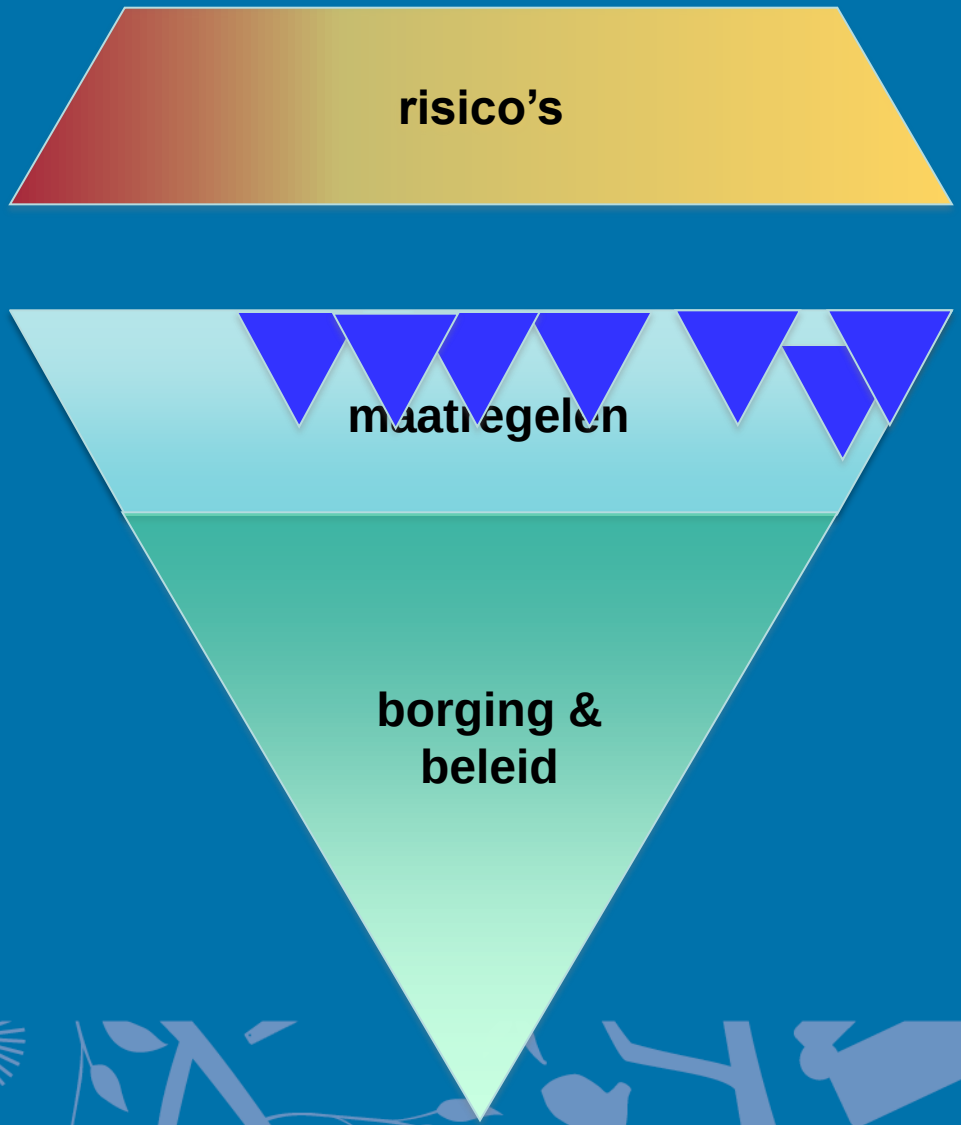
Lage risico's: 'first line of defence'

•Focus op maatregelen (niet zo zeer de borging van deze maatregelen en het vaststellen van het beleid waarop deze maatregelen gebaseerd zouden kunnen zijn)

•Focus op laaghangend fruit (maatregelen die zonder grote kosten of moeite kunnen worden geïmplementeerd en die de gebruiker niet erg in de weg zitten)

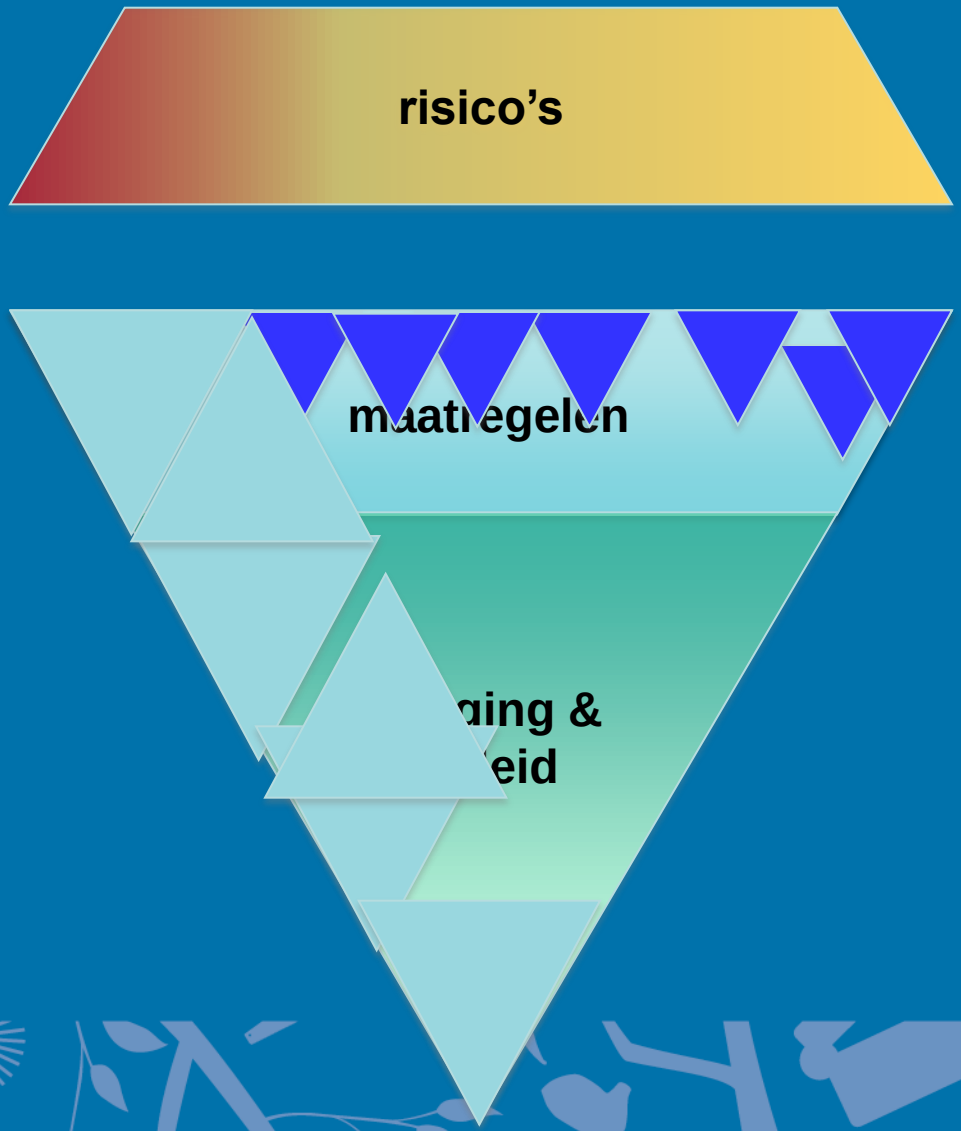
•Accepteer rest-risico's

lage risico's: focus op laaghangend fruit



niveau 2
(herhaalbaar
maar intuitief)

De nieuwe focus



De paarse krokodil…