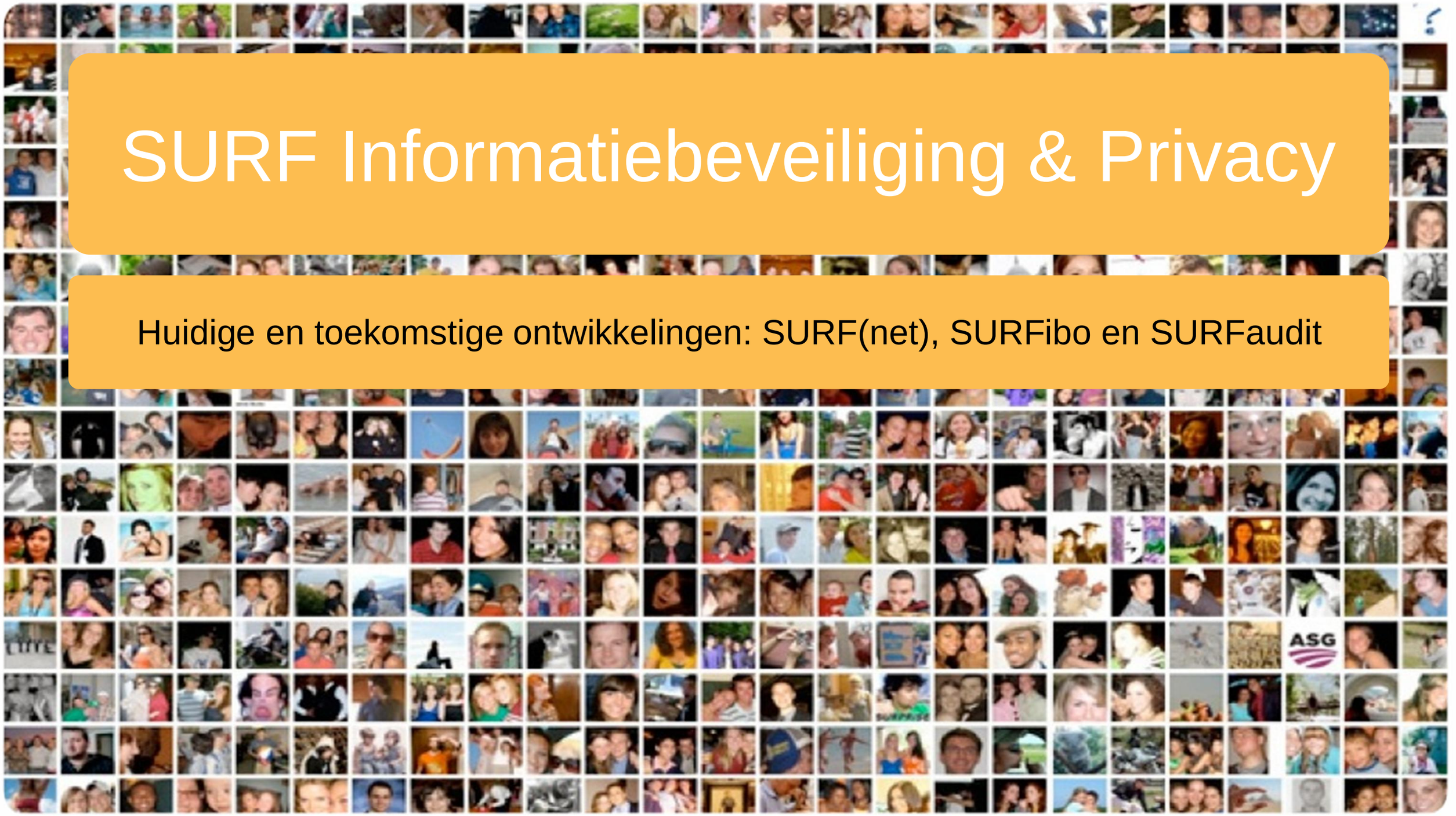
SURF Informatiebeveiliging & Privacy

Huidige en toekomstige ontwikkelingen: SURF(net), SURFibo en SURFaudit



Bart van den Heuvel, UM, SURFibo - april 2015

even voorstellen: Bart van den Heuvel

- Universiteit Maastricht
  - 1981 – 2003: Netwerkspecialist, UWDC
  - 2003 –> : CISO, vz. UM-Cert
- SURFnet
  - 1986 – 2005: ICO, SSC, HCP, SNM, HDB
  - 2003 –> : BVI, ICP, SSC, SNM, HDB
  - 2009 –> : lid SCIRT
- SURFibo → 2015 → SCIPR
  - 2002:SOHO –>2005:SURFibo (vz. 2010) –>2015……..
- SURF
  - 2014 –> : Lid Stuurgroep IB en Privacy

Credits: Alf Moens, Chloë Baartmans, Wilma Mossink,
Xander Jansen, CSY, SURFibo, SCIRT, Google, ….

amsix amsterdam internet exchange

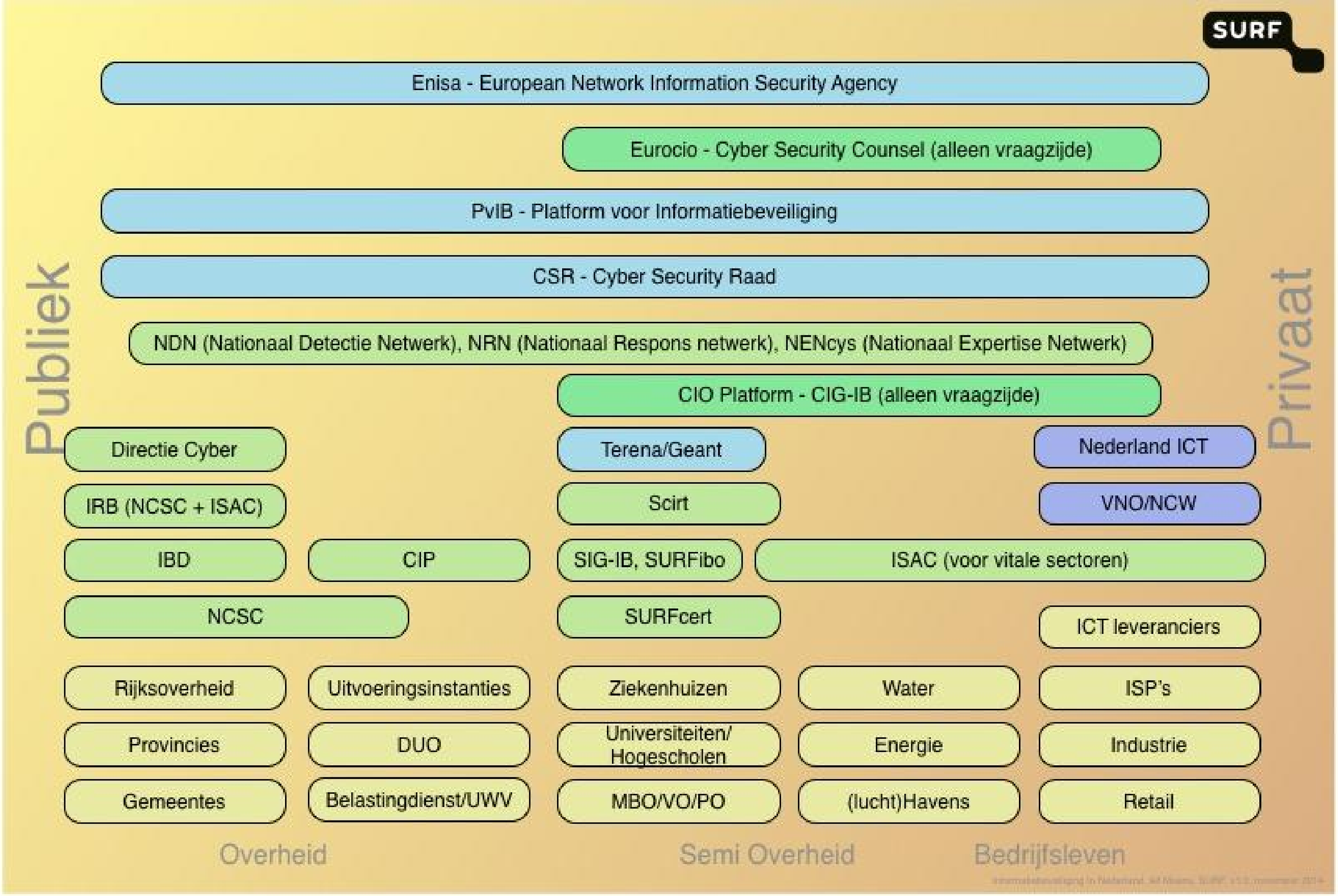
DNPA Dutch Hosting Provider Association

ISPConnect

nlnet Foundation

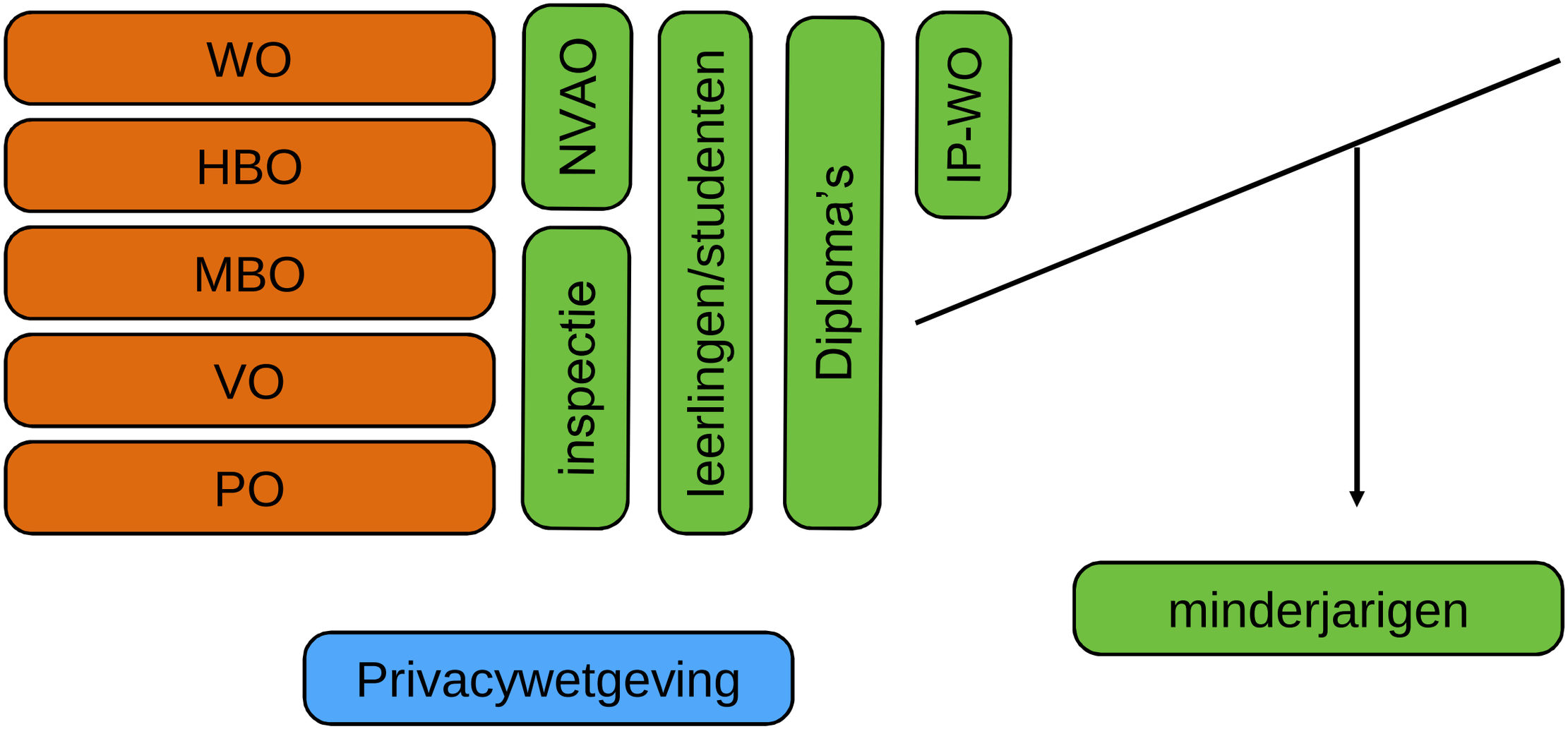
SIDN

SURF NET



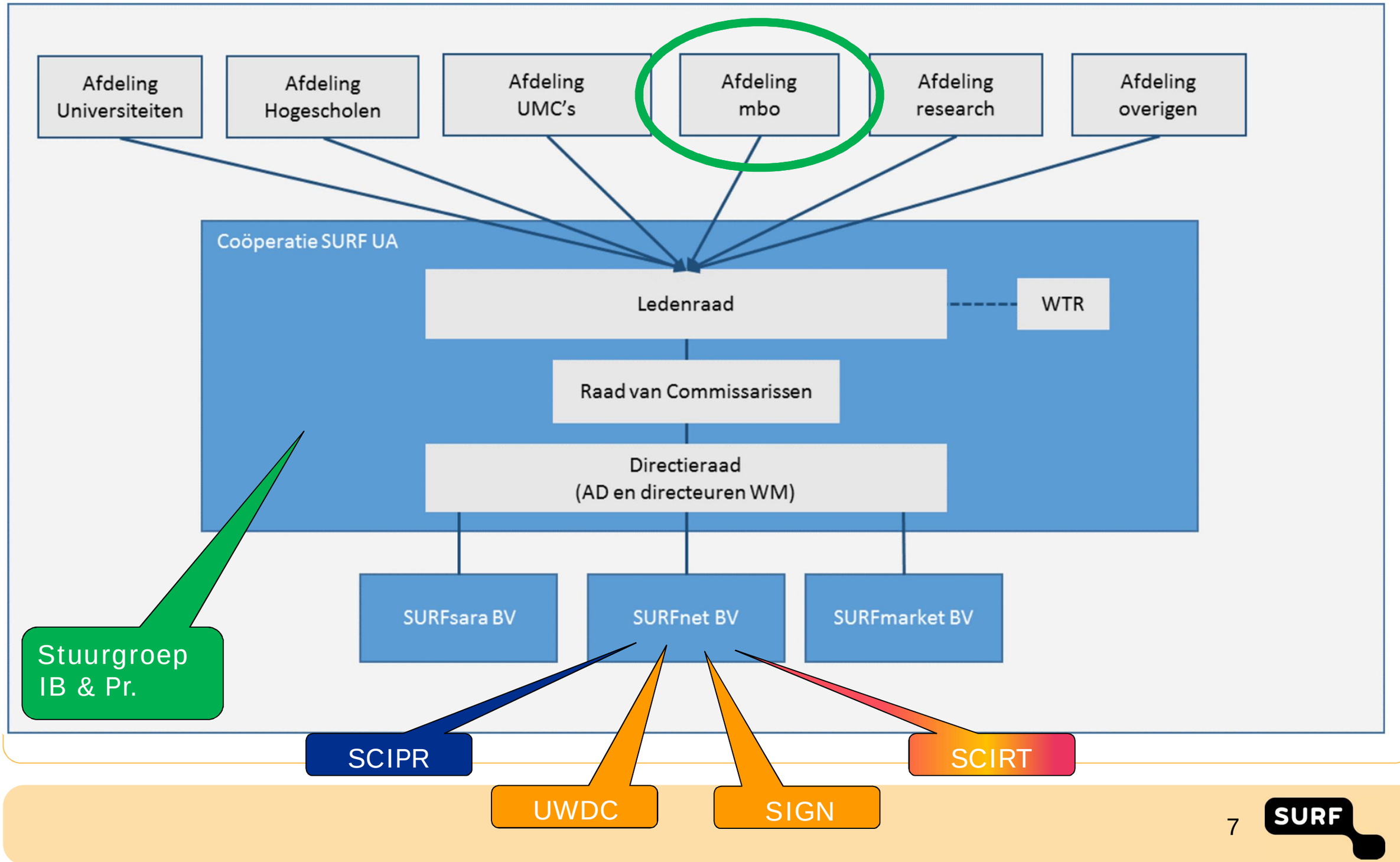
Informatiebeveiliging in Nederland (anno 2014)

Overeenkomsten en verschillen in de onderwijssectoren



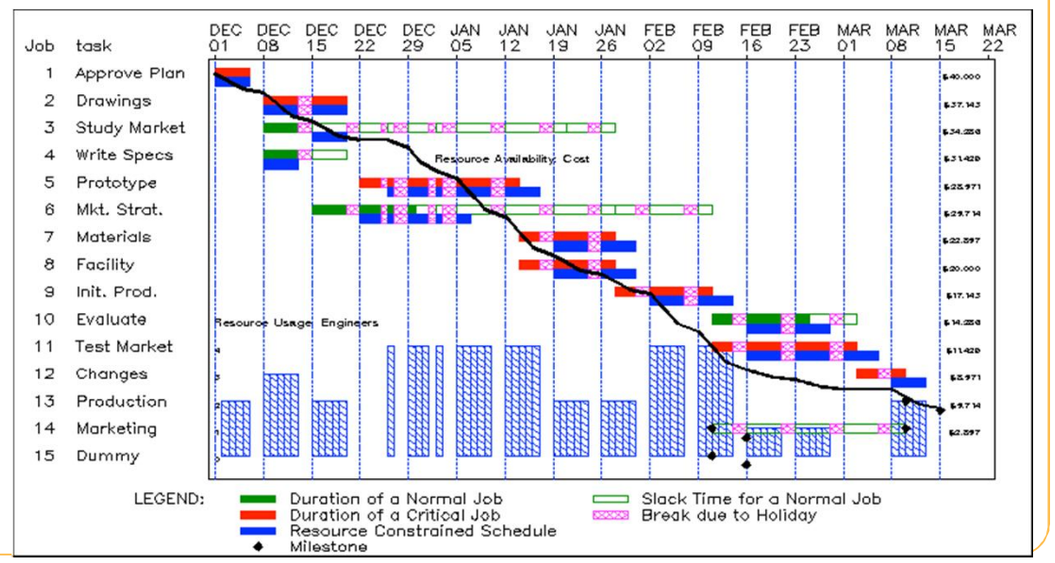
Structuur SURF per 1 januari 2015:

Coöperatieve Vereniging SURF

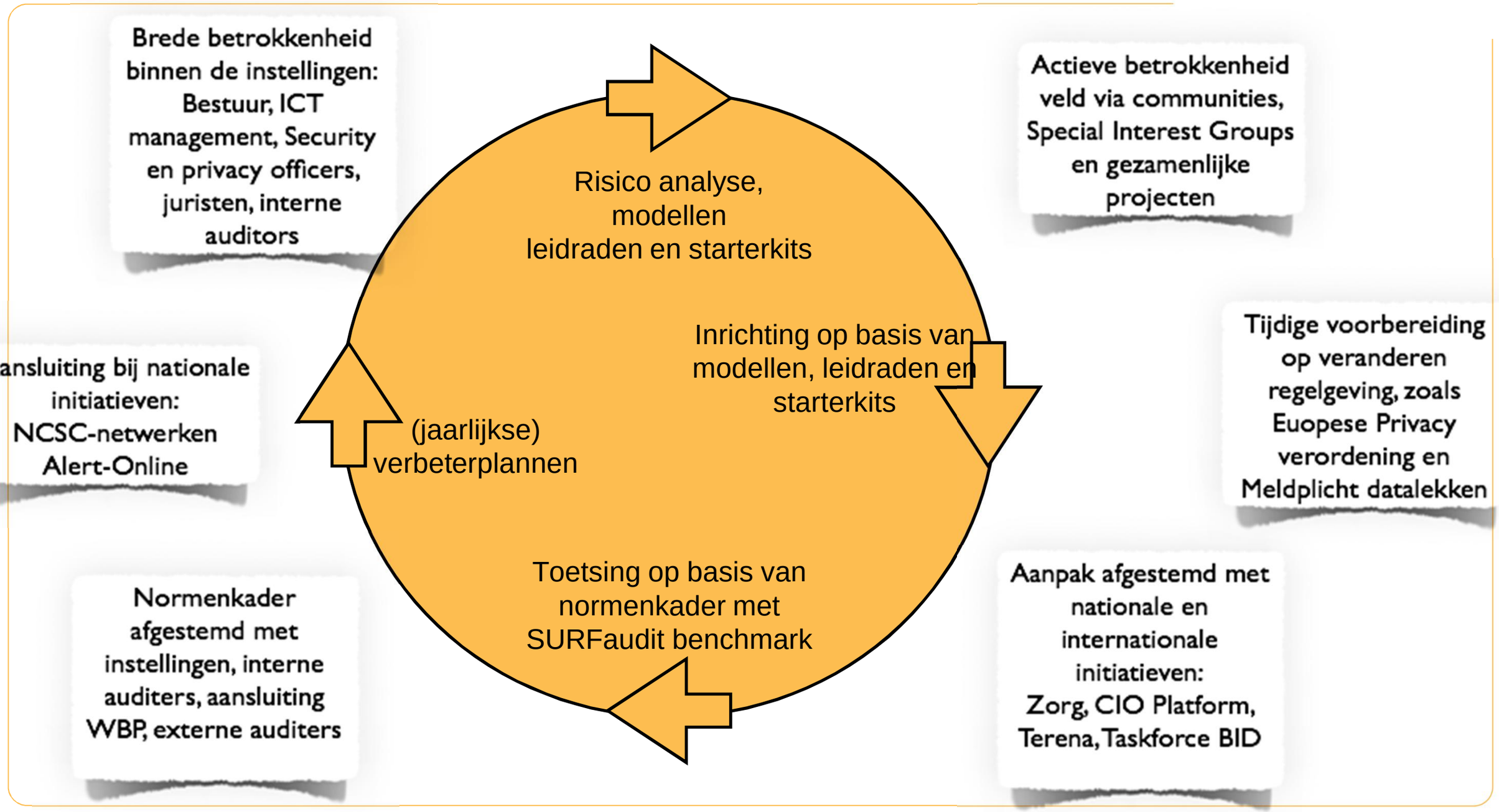


Innovatie programma’s 2015 - 2018

- P1: Verbindende Infrastructuren
- P2: Reken- en data infrastructuren
- P3: GF e-infrastructuur
- P4: Duurzame data
- P5: Onderwijs op Maat
- P6: Samenwerking aan ICT omgevingen voor onderzoek
- P7: Open Access
- P8: Betrouwbare en veilige omgeving
- P9: Efficiënte bedrijfsprocessen
- P10: Duurzaamheid



Informatiebeveiling in het HO



It’s all about Trust

Samenleving heeft groot vertrouwen in Onderwijs en Onderzoek*

Waar liggen we wakker van:
Financiele Risico’s
Cyberdreigingen
Privacy
Voldoende Kenniswerkers

Nerveuze maatschappij reageert excessief op in incidenten

Grootste dreigingen
Spionage (WO)
complexiteit infrastructuur
Wie/wat kan ik nog vertrouwen?
Vandalisme en Organised Crime

*Conclusie Commissie Vertrouwen en Integriteit in de Wetenschap KNAW 2013

Betrouwbare en Veilige Omgeving

Security en Privacy
Innovatie Deliverables in 2015

- Communities
  - –GAP analysis
  - –cross-organisationele community building
- Awareness
  - – strategie security intelligence
  - – awareness en marketingstrategie
  - – cybersave yourself,

    -> Game: Smart Secure Yourself
- Normen
  - – adoptie en compliance juridisch normenkader
  - – Best practice security en privacy standaarden
  - – Voorlichting juridisch normenkader
  - – Doorontwikkeling SURFaudit
- Diensten
  - – PvE security en privacy diensten
  - – Software defined security
  - – DDOS mitigatie
- Open Internet
  - – progress report/Papers

Communities

CYBERSAVE YOURSELF

CSY

Paypal

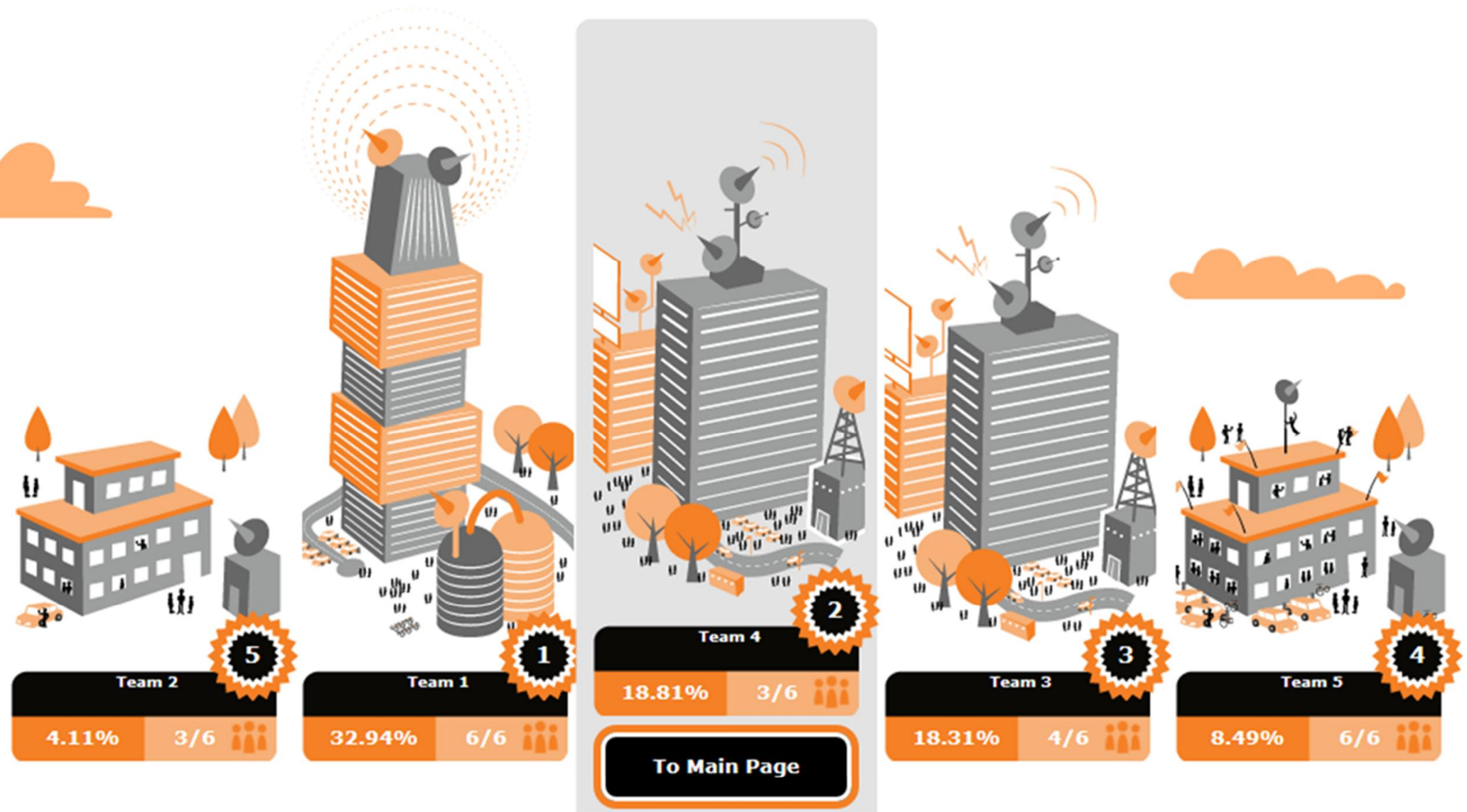
Yes, it was ph

Point and click
this is not the
right answers

The addres

CYBERSAVE YOURSELF

CSY



Team 2
5
4.11%
3/6

Team 1
1
32.94%
6/6

Team 4
2
18.81%
3/6

To Main Page

Team 3
3
18.31%
4/6

Team 5
4
8.49%
6/6

Juridisch Normenkader (Cloud) Sourcing

- Het juridisch normenkader stelt normen voor het hoger onderwijs qua vertrouwelijkheid, privacy, eigendom en beschikbaarheid ten aanzien van (cloud)leveranciers. Het bevat clausules die instellingen een stevige basis geven voor contracten met leveranciers.
- Bewerkersovereenkomst
- Passende maatregelen

  -> Compendium
- Auditverplichting

  -> of “recht op” ?

Framework InformatieBeveiliging in het Hoger Onderwijs — Intranetversie december 2014

HO Referentie Architectuur (SURF 2013)

Leidraad Informatie Beveiliging Architectuur

Starterkit InformatieBeveiliging

Model Beleid InformatieBeveiliging (update 2013/2014)

Information Security Management System: ISO 27001:2013 (vanaf sept 2014)

Baseline Informatie Beveiliging (Update 2014)	Leidraad AUP	Leidraad Classificatie (Update 2014 incl. LoA)	Leidraad Integriteit Code	Leidraad Functie-profiel (Update 2014 incl. FG)	Privacy (Initiatiefgroep)
Starterkit Identity Management	Starterkit RBAC	Starterkit Business Continuity Management	Leidraad veilig toetsen	IB in Projecten	Leidraad Responsible Disclosure
Leidraad Risico Management (PIA in 2014)	Leidraad Incident Management (Scirt)	Leidraad BYOD	CERT Starterkit	Cloud Normen-kader (Werkgroep)	Sourcing toolkit (SURF) Leidraad ->PvE

Veel implementatie voorbeelden van grote en kleine instellingen

Technische handreikingen (How-to's, FAQ's, etc.)

Normen-kader Informatie Beveiliging HO / SURFaudit (Peer Review 2014)

Klaar (ToDo) | beheer bij | in Progress | nog plannen

SURF

Privacy initiatief HO

- Juridisch kader
  - Raamwerk
  - Ist-Soll: Gap analyse
- PIA
  - Methodiek
  - voorbeelden: Studenteninfo; ….
- Privacy Beleid
  - Template
  - Leidraad

Samenwerken Werkt !!

Speciale thema's in SCIPR

- Data lekken

- Onderzoeks gegevens

- Gegevens minderjarigen

Het kind: speciale behandeling

- ❑ **Informatieplicht:** duidelijke en makkelijk te begrijpen taalgebruik
- ❑ **Recht om vergeten te worden**: bredere scope
- ❑ **Privacy by default**: kinderen assisteren waar mogelijk
- ❑ **Toestemming van ouders**: voor marketing doeleinden
- ❑ **Uitvoeren van een PIA**: in grote databestanden met gegevens van minderjarigen

Normenkader IB HO/MBO

1. Beleid & Organisatie:
- beveiligingsbeleid
- verantwoordelijkheden
- wetgeving
- incident management

2. Personeel, studenten en gasten:
- eisen en screening
- geheimhouding
- security awareness

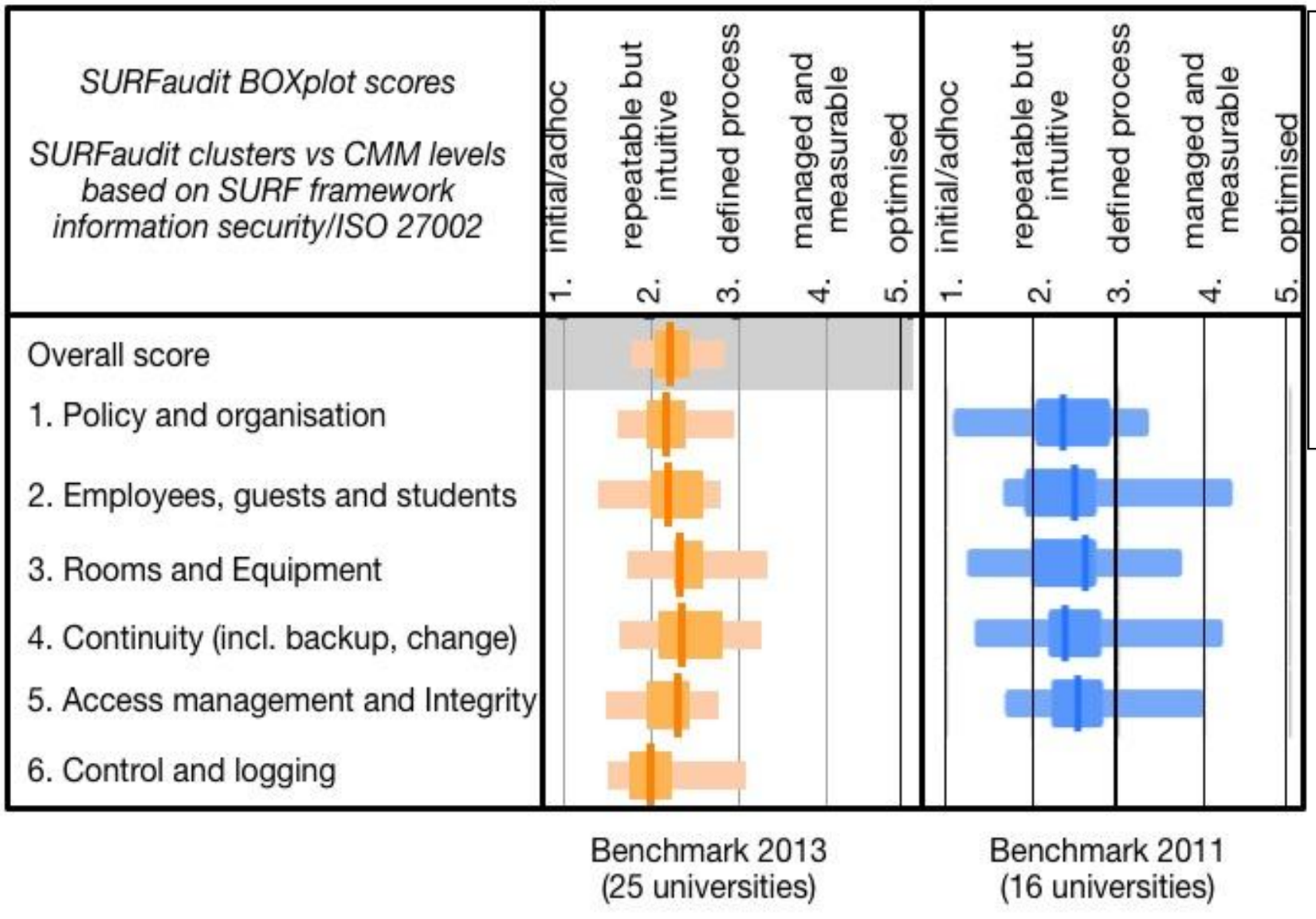
3. Ruimten & Apparatuur
- fysieke beveiliging
- nutsvoorzieningen
- e-waste

4. Continuiteit
- wijzigingsbeheer
- backup en restore
- continuiteitsplannen

5. Toegangbeveiliging & Integriteit
- toegangsbeleid
- userid’s en wachtwoorden

6. Controle & Logging
- (controle an) logging
- controle van systeemgebruik
- controle op technische naleving

SURFaudit - resultaten Benchmark 2013

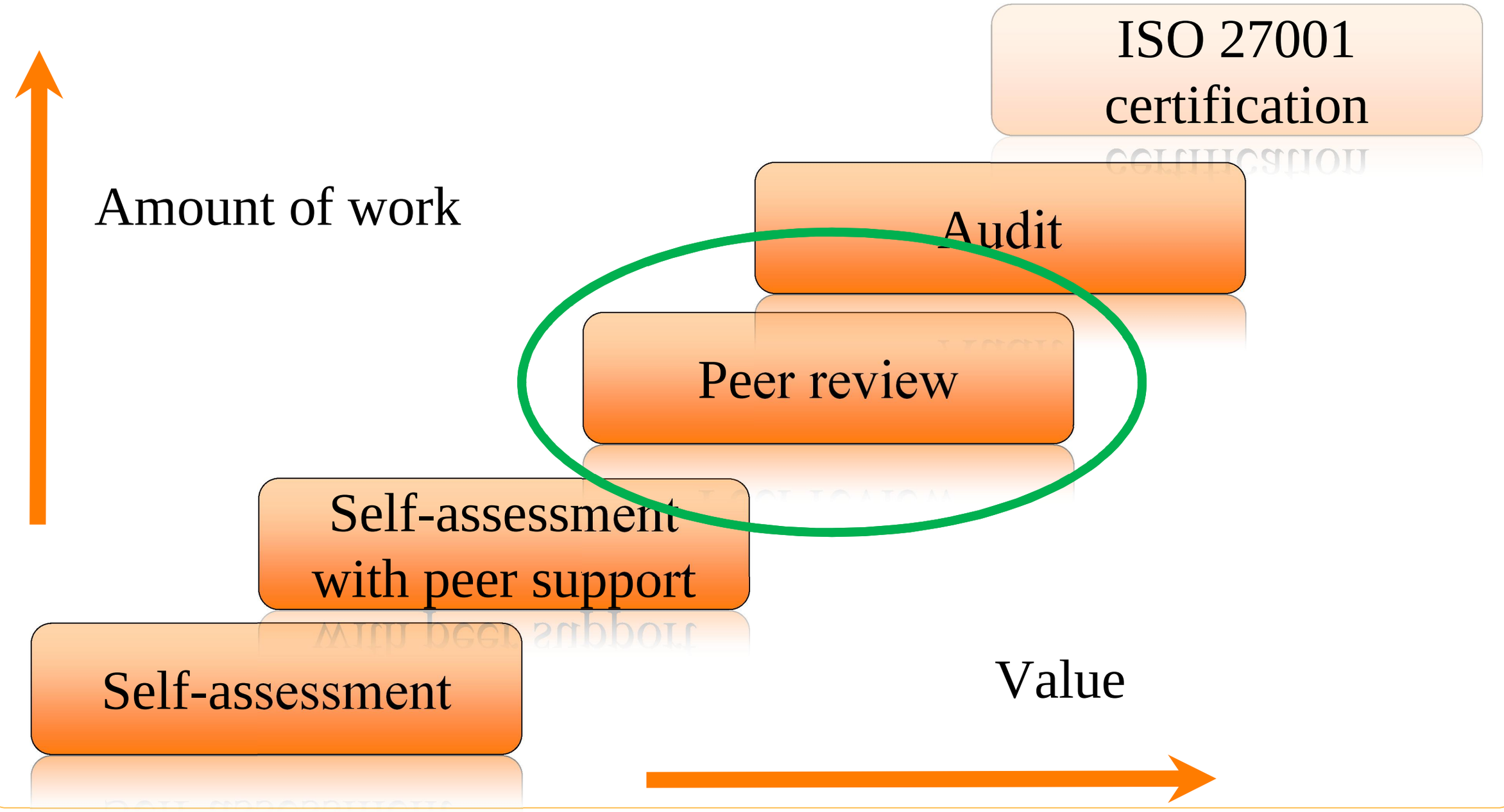


Scores in Benchmark 2013 lager

Redenen:
- *uitbreiding normenkader met privacy*
- *toevoeging evidence lijst*
- *kritischere metingen, serieuze aanpak*

Per instelling (resultaten 2013)
- *hoogste gemiddelde score 3,0*
- *laagste gemiddelde score 1,8*
- *3 instellingen met geen enkele 1*

Assessments en Audits



Cyberdreigingsbeeld 2014

- Inventarisatie belangrijkste risico's
- Bedoeld voor de bestuurstafel EN voor de security professional
- Hoofdlijnen en achtergronden
- Voorbeelden

- Gebaseerd op nationale en internationale onderzoeken aangevuld met eigen onderzoek (door Deloitte) in de sector

- Aangeboden aan CvB's

Dreigingsmatrix Sector Hoger Onderwijs en Wetenschappelijk Onderzoek

Dreigingen per actor		Dreiging		
Actor	**Vaardigheids niveau**	**Onderwijs**	**Onderzoek**	**Bedrijfsvoering**
Studenten	Laag tot Gemiddeld	Identiteitsfraude Manipulatie van data Verstoren ICT Bewust beschadigen imago		
Medewerkers	Laag		Identiteitsfraude Manipulatie van data Verstoren ICT	
Cybercriminelen	Gemiddeld tot Hoog	Verkrijging en openbaarmaking van data	Verkrijging en openbaarmaking van data Overname en misbruik ICT Spionage	Verkrijging en openbaarmaking van data Identiteitsfraude
Cyberonderzoekers	Hoog	Verkrijging en openbaarmaking van data Verstoren ICT	Verkrijging en openbaarmaking van data Verstoren ICT	Verkrijging en openbaarmaking van data Verstoren ICT
Staten	Zeer Hoog		Verkrijging en openbaarmaking van data Spionage Overname en misbruik ICT	
Commerciële bedrijven & Partner-instellingen	Laag tot Gemiddeld		Spionage	
Activisten	Laag tot Gemiddeld	Verstoren ICT Bewust beschadigen imago	Verstoren ICT Bewust beschadigen imago Overname en misbruik ICT	Verstoren ICT
Cybervandalen	Laag	Bewust beschadigen imago	Bewust beschadigen imago	

Legenda relevantie - *Bron: Cybersecuritybeeld Nederland (Nationaal Cyber Security Centrum, 2014)*

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

Bijstellen….

SURFaudit-6cluster-ISO27002-2013.xlsx

	Clusters HO	ISO27002 2013	Statements (totaal 83)	Mapping met Cyberdreigingsbeeld Sector HO Statement relevant voor Dreigingstype?								
				1	2	3	4	5	6	7		
Toevoegen ?	1.5 of 5.1?	6.1.2	Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.			X			?		2	
	1.6?	6.1.3	Contact met overheidsinstanties: Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.		?		X	?			3	Twijfel geval
	2.1	7.1.1	Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	?	X	X	X	X			5	
1	1.17	16.1.1	Er zijn voor leidinggevenden verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op	X	X	X	X	X	X	X	7	
2	1.18	16.1.2	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	X	X	X	X	X	X	X	7	
			Op informatiebeveiligingsincidenten behoort te									

It’s all about Risk

- Weten waar de waarde zit
- Wat moet beschermd worden?
- Wat is waardevol?
- Wat kost het als het mis gaat? en wat gaat er dan mis?

Opnieuw fraude, nu bij ROC A'dam

Nieuws

Door de groe
instellingen s
activisten
genoem

Studente
manipule
hacken
het rapp

Als er ov
persoons
toe geno
oplossin
niveaus

INFO SECURITY MAGAZINE

TSTC TSHUKUDU TECHNOLOGY COLLEGE

OME NIEUWS » BLOGS WHITEPAPERS AGENDA MAGAZINE » ABONNEREN

rije Universiteit Amsterdam besmet met ransomware

11 maart 2015 Nieuws

De Vrije Universiteit Amsterdam (VU) is getroffen door de Cryptolocker ransomware. Ongeveer 200 computers van de universiteit zijn in gijzeling genomen.

"Het Cryptolockervirus waart rond op ons netwerk", zegt Aukje Schep van de VU tegenover Security.nl. De malware zou zich hebben verspreid via e-mailbijlagen en bestanden op de computers ersleutelen. In ruil voor de encryptiesleutel eist de ransomware losgeld. Als tegenmaatregel zou de VU et netwerk afgelopen weekend op 'read-only' hebben gezet.

e impact van en schade door de ransomware lijkt dankzij goede backups mee te vallen. Vooralsnog zou ich niemand hebben gemeld die data is kwijtgeraakt. De bestrijding van de ransomware wordt bemoeilijk oor het feit dat Cryptolocker continu muteert. Hierdoor duikt de ransomware op allerlei plekken op, ook in ijvoorbeeld e-mailberichten van bekenden. Het advies geen e-mails van onbekenden te openen heeft du einig effect.

'C
g

Drie
jaar
vijfdeklassers verhoogden cijfers en verwijderden meldingen van absenties.

Dat meldt *RTV Noord-Holland* maandag. De leerlingen zijn geschorst.

2

mens.
ven alleen
mroep West.
n naar

De Juiste maatregelen.....

Awareness


Passwords are like
bubblegum
Strongest when fresh
Should be used by an individual, not a group
If left laying around, will create a sticky mess
© 2005 Native Intelligence.com


Passwords Are Like Underwear
Passwords are like underwear...
Change yours often.
Passwords are like underwear...
Don't share them with friends.
Passwords are like underwear...
The longer, the better.
Passwords are like underwear...
Be mysterious.
Passwords are like underwear...
Don't leave yours lying around.
I.T.S.A.

QUALYS® SSL LABS

Home Qualys.com Projects Contact

You are here: Home > Projects > SSL Server Test > sharepoint.hu.nl

SSL Report: [redacted]

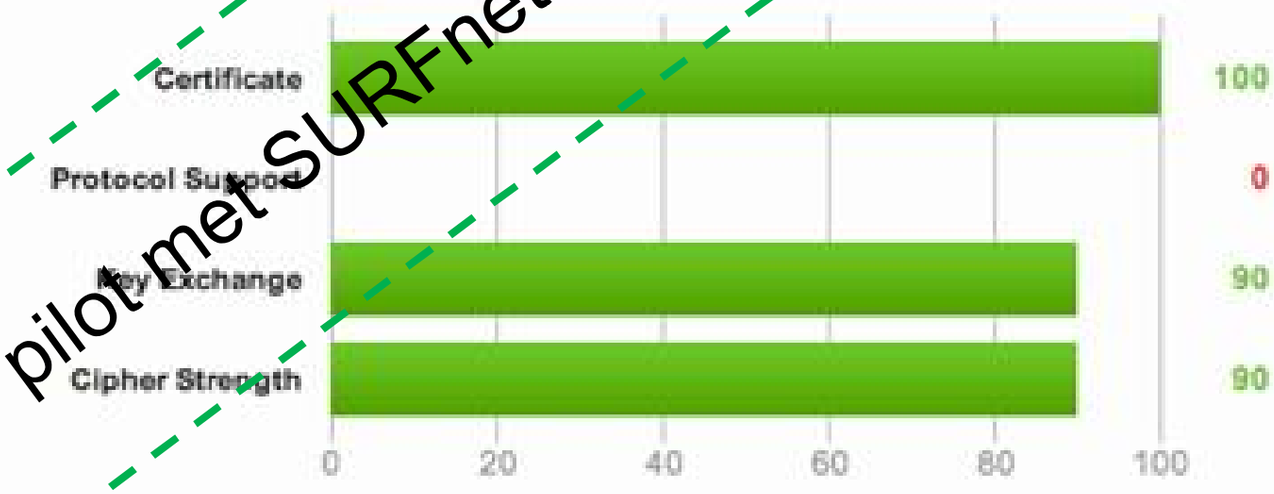
Assessed on: Wed Apr 17 15:38:40 UTC 2013 | HIDDEN | Clear cache

Scan Another >>

Summary

Overall Rating

F



Documentation: SSL/TLS Deployment Best Practices and SSL Server Rating Guide.

This server is vulnerable to MITM attacks because it supports insecure renegotiation. Grade set to F.

This server is easier to attack via DoS because it supports client-initiated renegotiation.

This server does not mitigate the BEAST attack. Grade capped to B.

(Distributed) Denial of Service

Xander Jansen / SURFcert

Beveiligingsconferentie SURFcert & SURFibo 13-2-2015

Wie wordt dan aangevallen?

- SURFnet heeft "permanente" filters geplaatst voor (op verzoek van):
- ~~17~~ 18 MBO instellingen
- 5 OSP’s (VO)
- 2 HBO’s
- 4 overige instellingen
- een tiental instellingen die incidenteel door de wasmachine gaan

Newsflash: Wasmachine wordt ook selfservice ?

Voorbereiding is het halve werk

- *Advies 1: stel een baseline vast en monitor uw infrastructuur*
- *Advies 2: instrueer de communicatie adviseur v*
  organisatie.
- *Advies 3: maak gebruik van*
- *Advies 4: inform* *tand en repressie*
  maatre *aanvallen en check de*
  co *rover.*
- *Adv* *k na over de incident response en fail-over*
  scenario's van de onlinediensten.
- *Advies 6: implementeer de voorgestelde (mitigerende) maatregelen aan het einde van deze factsheet.*

En laat zien dat je er iets aan doet
gebruik desnoods de schandpaal

Bron: NCSC Factsheet Continuïteit van onlinediensten

Dank voor uw aandacht !

Bart van den Heuvel
bart.vandenheuvel@maastrichtuniversity.nl

WHAT WE ! CAN DO

Referenties

- Juridisch normenkader voor cloud computing
- https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html
- Richtsnoer beveiliging persoonsgegevens
- https://cbpweb.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013
- Hoe?zo! Informatiebeveiliging
- http://www.sambo-ict.nl/wp-content/uploads/2014/09/KNS_Informatiebeveiliging_FINAL4A.pdf
- Cyberdreigingsbeeld HO
- https://www.surf.nl/nieuws/2014/11/handvatten-om-cybersecurity-instellingen-te-verbeteren.html
- Security en privacy @ SURF
- https://www.surf.nl/themas/beveiliging
- https://www.surf.nl/themas/digitale-rechten/privacy/implementatie-algemene-verordening-gegevensbescherming-avg/index.html