Informatiebeveiliging in het Hoger Onderwijs

Compliance and Control

SAMBO-ICT - 16 januari 2014 - Alf Moens

Wat ga ik u brengen?

- Framework Informatiebeveiliging, best practices uit het onderwijs
- Normenkader voor informatiebeveiliging: Wat moet een onderwijsinstellingen tenminste geregeld hebben?
- Tools voor Compliance en Control: SURFaudit
- En… hoe je dit allemaal organiseert

WhoAmI

- Alf Moens (alf.moens@surf.nl)
- Coordinator Informatiebeveiliging & Privacy - SURF
  - SURF werkmaatschappijen en coordinatie HO
- Parttime docent HU
- Vice voorzitter Platform voor Informatiebeveiliging
- (Security Manager TU Delft 2003-2012)
- MISM / Lead Auditor ISO 27001 / ISO 27005 Risk Manager

SURF

ICT & Onderzoek

BIG Data spionage

ICT & Onderwijs

Veilig Toetsen/ Toetsinfrastructuur

ICT & Bedrijfsvoering

Compliance Privacy & juridisch organisatie

SURFnet

SURFcert

Federatie/ Conext

GIGAport

SURFworks

SURFnet/ Kennisnet

SURFmarket

Software

Diensten

SURFsara

SURFshare

Studielink

Studiekeuze123

Deelnemingen

eScience

SANS

PI.lab

Science

Radboud

VU

UvA

Programma BIS

SURFaudit

Privacy

IDM

Disseminatie

Taskforce Cloud

Cloud First

Regie in de cloud

SURF projecten

IBP @ SURF

Kantoor

SION

Onderwijsidentiteit / IAA

Stuurgroep Informatiebeveiliging & Privacy Hoger Onderwijs (IBHO)

Bestuurders

Universiteiten

Hogescholen

UMC's

Wetenschappe-lijke instellingen

MBO's, bibliotheken, overigen

CIOberaad

CvDUR

COMIT

H-BOSS

CVUAD

KAAIWO

SIG IDM

SURFibo

Framework IB HO

netwerken

SCIRT

Trainingen

Internationaal

Cloud

Terena

TF-csirt

EuroCio Cyber Security Counsil

Externe partijen

PvIB

CPNI

Kennisnet

Stuurgroep KIN

CIO Platform / SIG / Bestuurscommissie

Overheid

NCSC

BID

CBP

Inspectie

OCW

CIP

IBP @ SURF, versie 1.8, augustus 2013, Alf Moens

Higher Education in NL

- 14 Academic universities
- 45 Universities of Professional Education
- 8 Academic Hospitals
- 7 other (research, National Library etc.)
- X * 10 GBps network
- 658.000 students (2011)

Waarom beveiligen?

Compliance and Control

- Vertrouwen noodzakelijk voor intensieve samenwerking
- Wettelijke regels:
  - Privacy wetten, worden flink aangescherpt met de EPV (vanaf 2014)
  - Telecom wet,Wetten computercriminilateit
  - Bewaarplichten
- Accountantscontrole
  - verantwoording voor jaarrekening
  - verantwoording voor subsidie projecten
  - substantieel belang (boetes EPV)
- Aansluitvoorwaarden
  - SURFnet, SURFconext
- Contractuele bepalingen
  - opdrachtgevers
  - internationale partners
- Open data?
- Publieke opinie en IMAGO

Hoe realiseer je Compliance en Control?

- Commitment
- Normenkader IB
- Meten met SURFaudit
- Framework IB&P HO

Contractuele bepalingen

- Onderzoekspartners stellen eisen aan opslag en verwerking van gegevens
- Voor, tijdens en na het onderzoek
- Wat vragen/eisen opdrachtgevers/partners?
  - informele inventarisatie bij een van de universiteiten

CBP publiceert Onderzoek Hogescholen

Hogescholen verbeteren beveiliging studentgegevens na onderzoek CBP
Onderzochte hogescholen moeten nog enkele overtredingen beëindigen

Persbericht, 7 februari 2013

Hogeschool Utrecht (HU) en Hogeschool van Arnhem en Nijmegen (HAN) hebben onvoldoende beveiligingsmaatregelen getroffen om de studentgegevens in interne informatiesystemen te beveiligen tegen verlies of onrechtmatige verwerking. Dat concludeert het College bescherming persoonsgegevens (CBP) na onderzoek. De hogescholen overtreden hiermee de Wet bescherming persoonsgegevens (Wbp). De beveiliging van studentgegevens zoals studieresultaten, foto's, informatie over leningen of notities van decanen is juist van groot belang. Studenten moeten erop kunnen vertrouwen dat hun persoonsgegevens bij hun school in goede handen zijn en dat hun privacy is gewaarborgd. Scholen moeten voorkomen dat onbevoegden persoonsgegevens zoals cijfers kunnen wijzigen in het systeem. Beide hogescholen hebben naar aanleiding van het CBP-onderzoek maatregelen genomen om de informatiesystemen beter te beveiligen. Bij de HU missen nog meerdere beveiligingsmaatregelen. De HAN heeft nog één overtreding openstaan.

http://www.cbpweb.nl/Pages/pb_20130207-beveiliging-studentgegevens-hogescholen.aspx

Informatiebeveiliging

Informatiebeveiliging

Informatiebeveiliging

PRIVACY

Informatiebeveiliging

PRIVACY

CYBERanything

Informatiebeveiliging

PRIVACY

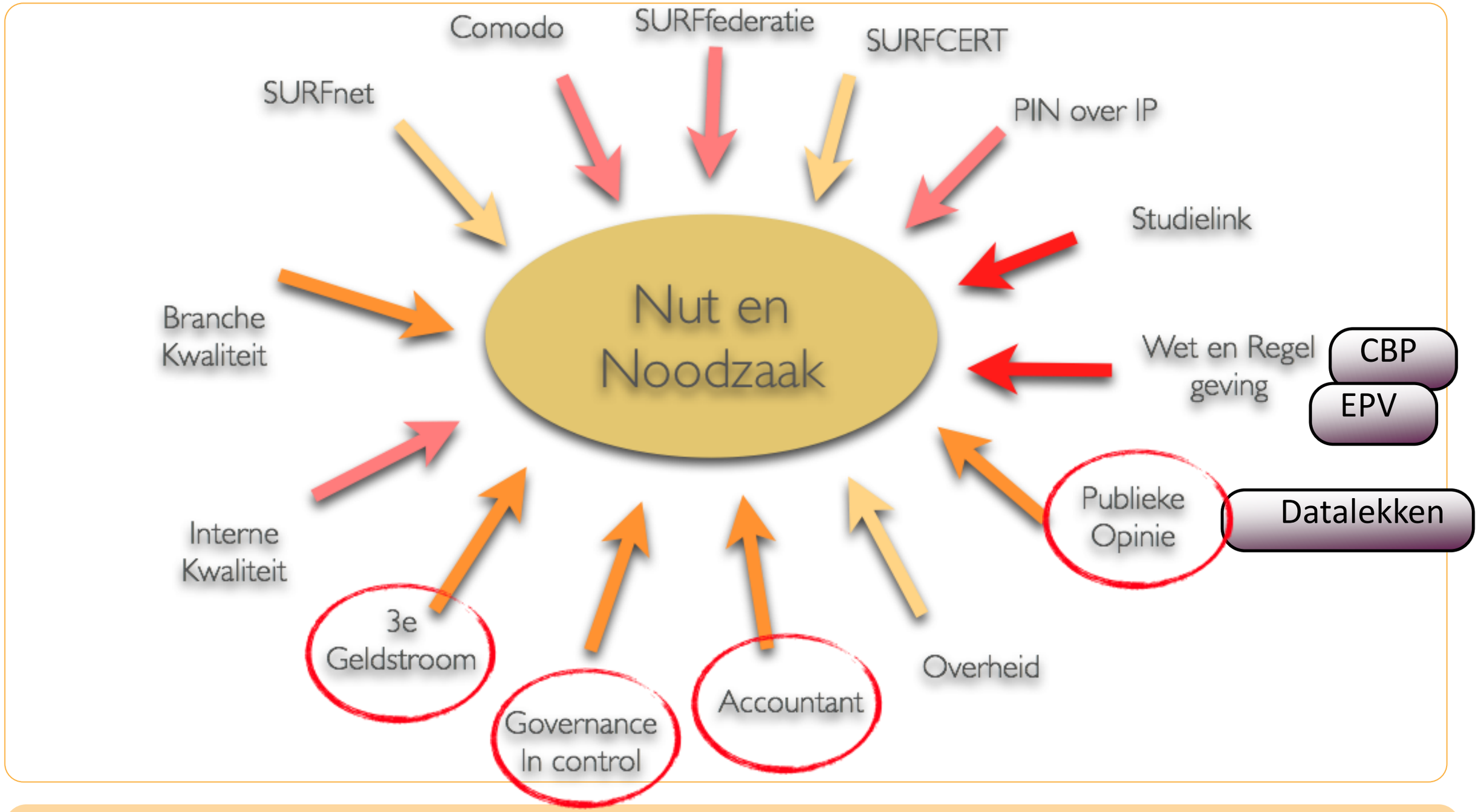
Informatiebeveiliging

CYBERanything

- Neelie Kroes:
- Stef Blok:

- Informatiebeveiliging prominente plaats in iStrategie

Waarom Beveiligen?



ARCTIC
WHITE

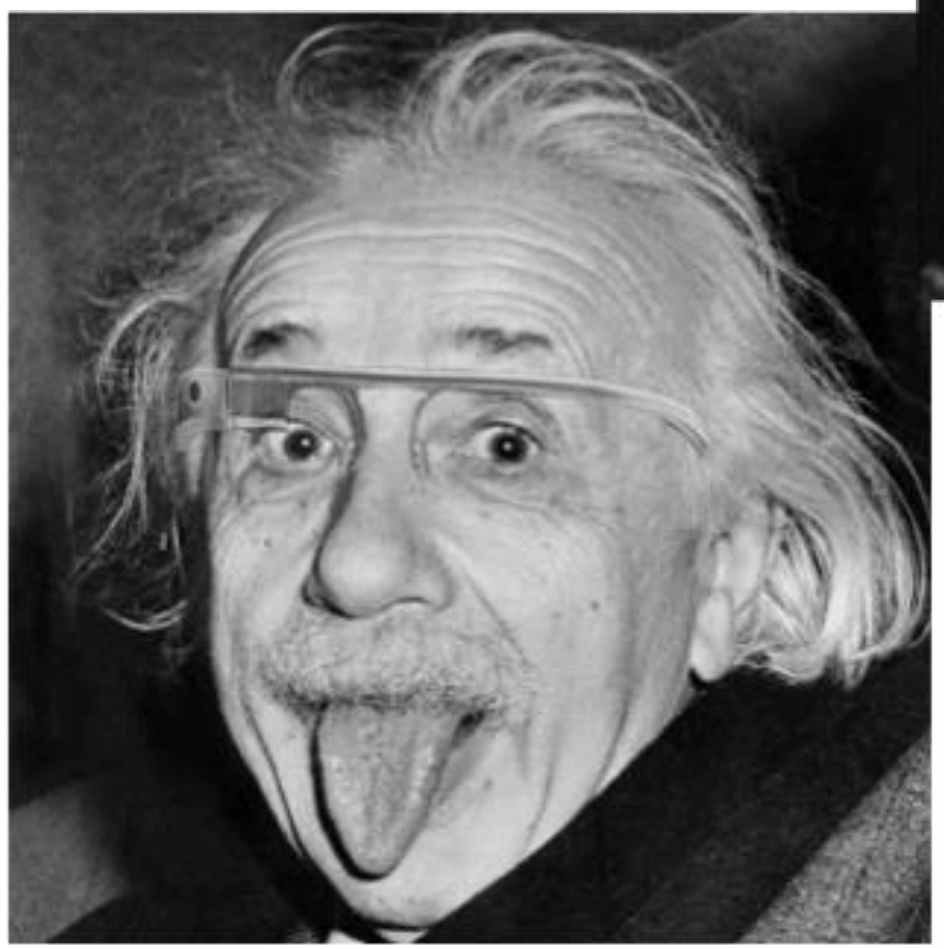
JET
BLACK

CHERRY
RED

ARCTIC
WHITE

BLACK

RED



2007

2008

2009

2010

2011

roefmetingen maturity
nformatiebeveiliging

Meting
Identity Management
voor SURFfederatie

BIM: metingen komen bij
elkaar

tegreerde aanpak

Bestuurlijk, CIO, ICT,
Beveiliger

draagvlak v
normen

draagvlak voor
methode en kosten

Mixed
financiering?

rtificering
udielink

normen voor SIM
en IdM

Programma van
eisen

Metingen maturity
informatiebeveiliging

normen toetsen

Meting
Incident Management
voor CERT vorming

eferentiekader IB

lot
SURFaudit

Selectie
meetpartijen

Scenario(‘s)
testen

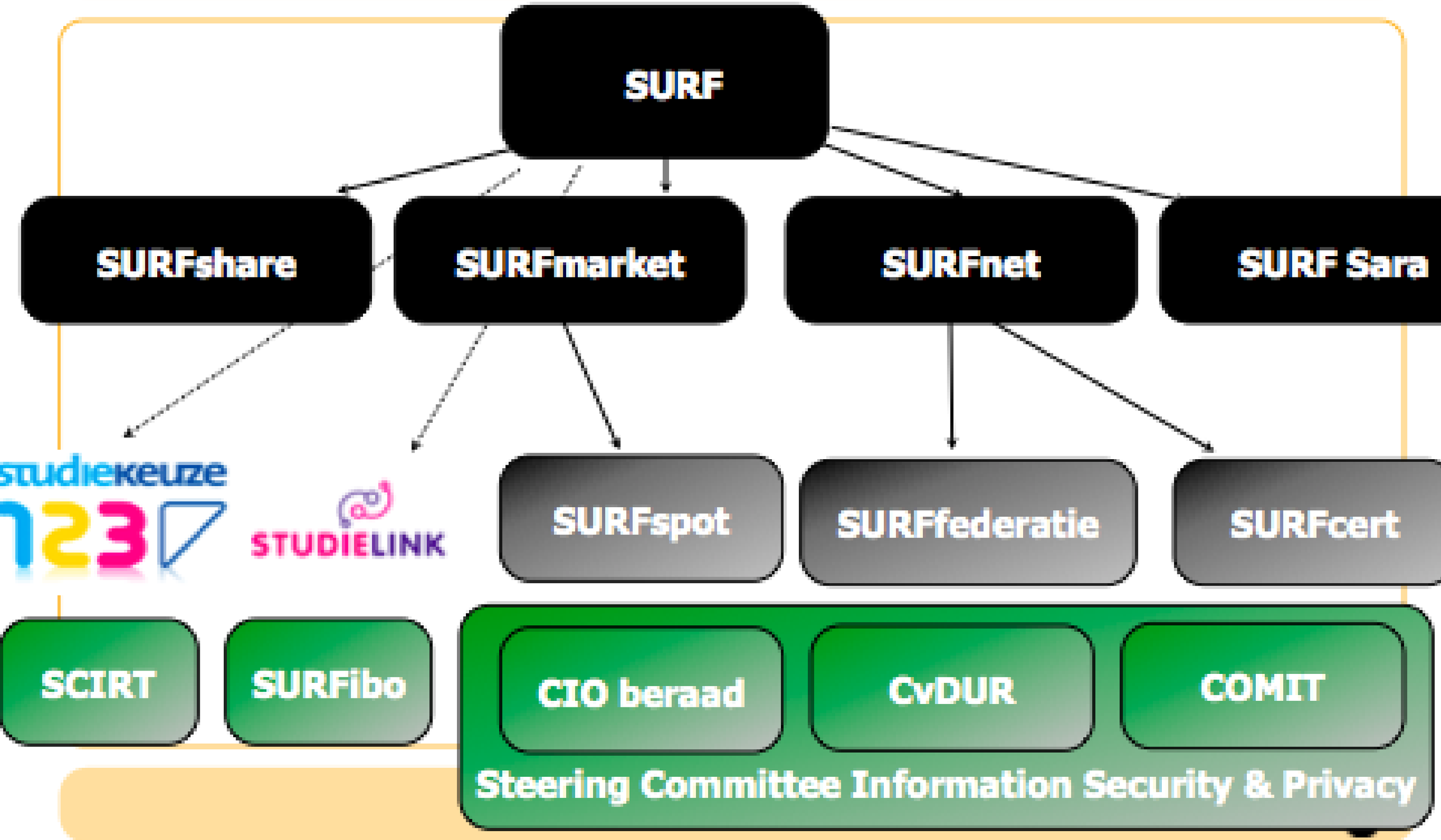
De markt meet,?
borging bij SURF

- de start van SURFaudit...

SURFaudit

- 2011: bencharkmeting met 16 instellingen
  - normenkader 2011, 5 clusters
- 2013: benchmarkmeting met
  - 11 a 12 universiteiten
  - 15 hogescholen
  - normenkader 2013, 6 clusters, uitbreiding met privacy
- 2014: opzetten onafhankelijk beoordeling met peer-auditing

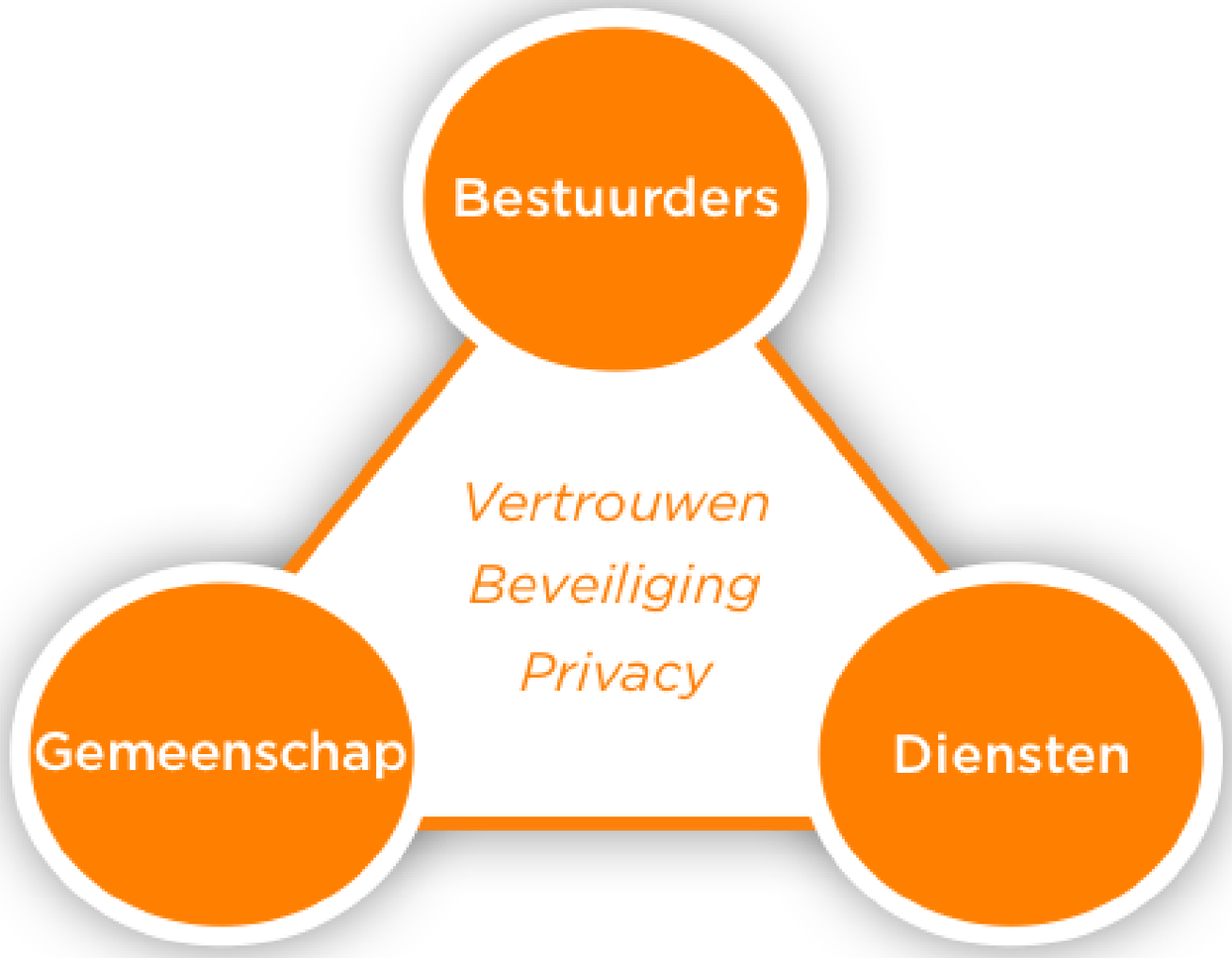
How Things Are Organised



Informatiebeveiliging van project naar proces

Informatiebeveiliging: Hoe komen we verder?

- Samenwerken
- Delen
- Ondersteunen



SURF

- ICT & Onderzoek
  - BIG Data spionage
- ICT & Onderwijs
  - Veilig Toetsen/ Toetsinfrastructuur
- ICT & Bedrijfsvoering
  - Compliance Privacy & juridisch organisatie

SURFnet

- SURFcert
- Federatie/ Conext
- GIGAport
- SURFworks
- SURFnet/ Kennisnet

SURFmarket

- Software
- Diensten

SURFsara

SURFshare

Stuurgroep Informatiebeveiliging & Privacy Hoger Onderwijs (IBHO)

Studielink

Studiekeuze123

Deelnemingen

- eScience
- SANS

Science

- PI.lab
- Radboud
- VU
- UvA

Programma BIS

- SURFaudit
- Privacy
- IDM
- Disseminatie

Taskforce Cloud

- Cloud First
- Regie in de cloud

SURF projecten

- IBP @ SURF
- Kantoor

SION

- Onderwijsidentiteit / IAA

Bestuurders

- Universiteiten
- Hogescholen
- UMC's
- Wetenschappelijke instellingen
- MBO's, bibliotheken, overigen

CIOberaad

- CvDUR
- COMIT
- H-BOSS
- CVUAD
- KAAIWO
- SIG IDM

SURFibo

- Framework IB HO
- netwerken

SCIRT

- Trainingen

Internationaal

- Cloud
- Terena
- TF-csirt
- EuroCio Cyber Security Counsil

Externe partijen

- PvIB
- CPNI
- Kennisnet
- Stuurgroep KIN
- CIO Platform / SIG / Bestuurscommissie

Overheid

- NCSC
- BID
- CBP
- Inspectie
- OCW
- CIP

IBP @ SURF, versie 1.8, augustus 2013, Alf Moens

security communities

SURF CERT

SCIRT forum for operational security

SURF IBO

Framework InformatieBeveiliging in het Hoger Onderwijs — Intranetversie december 2013

HO Referentie Architectuur (SURF 2013)

Leidraad Informatie Beveiliging Architectuur

Normen-kader Informatie Beveiliging HO / SURFaudit (SURFaudit 2013)

Starterkit InformatieBeveiliging

Model Beleid InformatieBeveiliging
(update 2013/2014)

Information Security Management System: ISO 27001:2013 **(invoeren 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
Starterkit Identity Management	Starterkit RBAC	Starterkit Business Continuity Management	Leidraad veilig toetsen	IB in Projecten	Leidraad Responsible Disclosure **(2013/2014)**
Leidraad Risico Management **(PIA in 2014)**	Leidraad Incident Management (Scirt)	Leidraad BYOD	CERT Starterkit	Cloud Normen-kader **(SURF 2013/14)**	Sourcing toolkit **(SURF / CIO-beraad 2012)**

Veel implementatie voorbeelden van grote en kleine instellingen

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

Klaar **(ToDo)**

beheer bij derden

in Progress

nog plannen

Informatiebeveiliging: Hoe staan we er voor?

- In 2008:
  - IT beveiliging en fysieke beveiliging goed op orde
  - Universiteiten net iets verder dan hogescholen
- In 2011:
  - geen grote verschillen meer
  - techniek nog steeds op orde
- In 2013
  - Eerste hogescholen maken serieus werk van compliance aangestuurd vanuit bestuurlijk niveau

SURFaudit consists of

- a control framework,
  - based on ISO27002, a selection of controls that at least must be implemented in Higher Education.
  - in 2013 expanded based on clearified privacy regulations
- a scoring scale and
  - 5 levels based on CMM
- a benchmarktool,
  - with build in scoring, explanation, required evidence, reporting and comparison
- with broad commitment from security officers, ICT managers, CIO's and boardmembers of the institutions
- But still voluntary.
- Same methods and tools are used in healthcare (hospitals) and amongst members CIO Platform (major Dutch companies).
- SURFaudit is part of the Information Security Framework HO-NL.

- *It's a combination of organisational, personell and technical controls!*

Normenkader 2013

Cluster	ISO 27002	Toetselement
1 Beleid & Organisatie	5.1.1	Beleidsdocument voor informatiebeveiliging
	5.1.2	Evaluatie en actualisering
	6.1.1	Bestuurlijke verankering
	6.1.3	Toewijzing en vastlegging van verantwoordelijkheden voor I
	10.8.1	Beleid voor gegevensuitwisseling
	10.8.2	Overeenkomsten
	12.1.1	Analyse en specificatie van beveiligingseisen
	15.1.4	Bescherming van persoonsgegevens
	13.1.1	Rapporten beveiligingsincidenten
	13.2.1	Verantwoordelijkheden en procedures incidentafhandeling.
2 Personeel, studenten en gasten	8.1.3	Arbeidscontract/voorwaarden
	8.2.2	Bewustwording, opleiding en training voor informatiebeveiliging
	8.3.3	Blokkering van toegang
3 Ruimten & Apparatuur	9.1.2	Fysieke toegangsbeveiliging
	9.1.5	Werken in beveiligde ruimten
	9.2.4	Onderhoud van apparatuur
	11.3.3	Clear desk en clear screen policy

Cluster	ISO 27002	Toetselement
4 Continuïteit	10.1.2	Beheer van wijzigingen
	10.4.1	Maatregelen tegen kwaadaardige programmatuur
	10.5.1	Reservekopieën
	14.1.1	Het proces van continuïteitsbeheer
	14.1.2	Bepaling van de continuïteitsstrategie
	14.1.3	Ontw. en impl. continuïteitsvoorzieningen & –plannen
	14.1.4	Structuur voor continuïteitsplannen
5 Toegangsbeveiliging	11.1.1	Toegangsbeleid
	10.8.4	Geautomatiseerde gegevensuitwisseling (tussen systemen)
	10.9.2	Transacties "on line" (tussen personen en systemen)
	11.2.1	Registratie van gebruikers (is incl autorisatie)
	11.5.2	Gebruikersidentificatie en authenticatie
	11.4.6	Beheersmaatregelen voor netwerkverbindingen
	11.4.5	Scheiding van netwerken
	11.2.2	Beheer van speciale bevoegdheden
	11.5.1	Inlogprocedures
	11.3.1	Gebruik van wachtwoorden en authenticatiemiddelen
	11.6.1	Beperken van toegang tot informatie
	11.6.2	Isoleren gevoelige systemen

Tabel 1: Normenkader SURFaudit

Uitbreiding 2013 opb richtsnoer WBP	
10.10	Logging en Controle
12.2	Correcte verwerking in toepassingssystemen
12.6	Beheer van technische kwetsbaarheden
6.1.5	Geheimhoudingsovereenkomsten
12.3	Encryptie en hashing
9.2.6	Omgang met e-waste
15.2.1	Controle op naleving binnen de organisatie
15.2.2	Controle op technische naleving
12.5.5	code review
10.3.2	Test van nieuwe en gewijzigde informatiesystemen
Bij cloud/uitbesteding:	
6.2.3	beveiligingseisen in bewerkersovereenkomst
7.2	differentiatie van verwerkte persoonsgegevens (classificatie
10.2.2	controle en beoordeling van dienstverlening
13.1.2	Beoordeling en afhandeling van incidenten en lekken
10.2.3	beheer van wijzigingen in de dienstverlening

Normenkader Hoger Onderwijs Clusters

Zes Clusters:

1. Beleid en Organisatie
2. Medewerkers, studenten en gasten
3. Ruimten & Apparatuur
4. Continuiteit
5. Toegangsbeveiliging en integriteit
6. Logging en controle

Normenkader Hoger Onderwijs: ISO27002 normen

Zes Clusters:

1. Beleid en Organisatie
2. Medewerkers, studen
3. Ruimten & Apparatuu
4. **Continuiteit**
5. Toegangsbeveiliging e
6. Logging en controle

Norm	ISO 27002:2007
Wijzigingsbeheer	10.1.2, 10.2.3
Backup & Restore	10.5.1
Beheer kwetsbaarheden	12.6.1
Bedrijfscontinuiteit	14.1 (alle)

Normenkader Hoger Onderwijs: Bewijsmateriaal

Zes Clusters:

1. Beleid en Organisatie
2. Medewerkers, studen
3. Ruimten & Apparatuu
4. **Continuiteit**
5. Toegangsbeveiliging e
6. Logging en controle

Norm	ISO 27002:2007
Wijzigingsbeheer	**10.1.2**, 10.2.3
Backup & Restore	
Beheer kwetsbaa	
Bedrijfscontinuite	

Opzet:
1. Beschrijving van de organisatie mbt OTAP;
2. Kopie procesbeschrijving "change management proces";
Bestaan (maakt onderscheid in incidenten, kleine - en grote spoedwijzigingen):
1. Kopie van informatie waaruit blijkt dat de organisatie conf heeft gewerkt. Te denken aan:
- Kopie gehanteerd RFC formulier (lijncontrole); inclusief take verantwoordelijkheden rondom CM en ontwep documentati
- Kopie impactanalyse van de wijziging (lijncontrole);
- Kopie acceptatieformulier , inclusief testuitkomsten (lijncon
- Schermprint van de change die van ontwikkelomgeving naa wordt geimplementeerd (lijncontrole)
- Kopie eerste meldingen bij in productie inname en trainingc
2. kopie van informatie waaruit blijkt dat de organisatie cont uitgevoerd op spoedwijzigingen.

Zowel gebruikers als beheersomgeving infrastructuur.

Different types of assessments and audits

ISO 27001 certification

Amount of work

Audit

Peer Audit

Self-assesment with peer support

Self-assesment

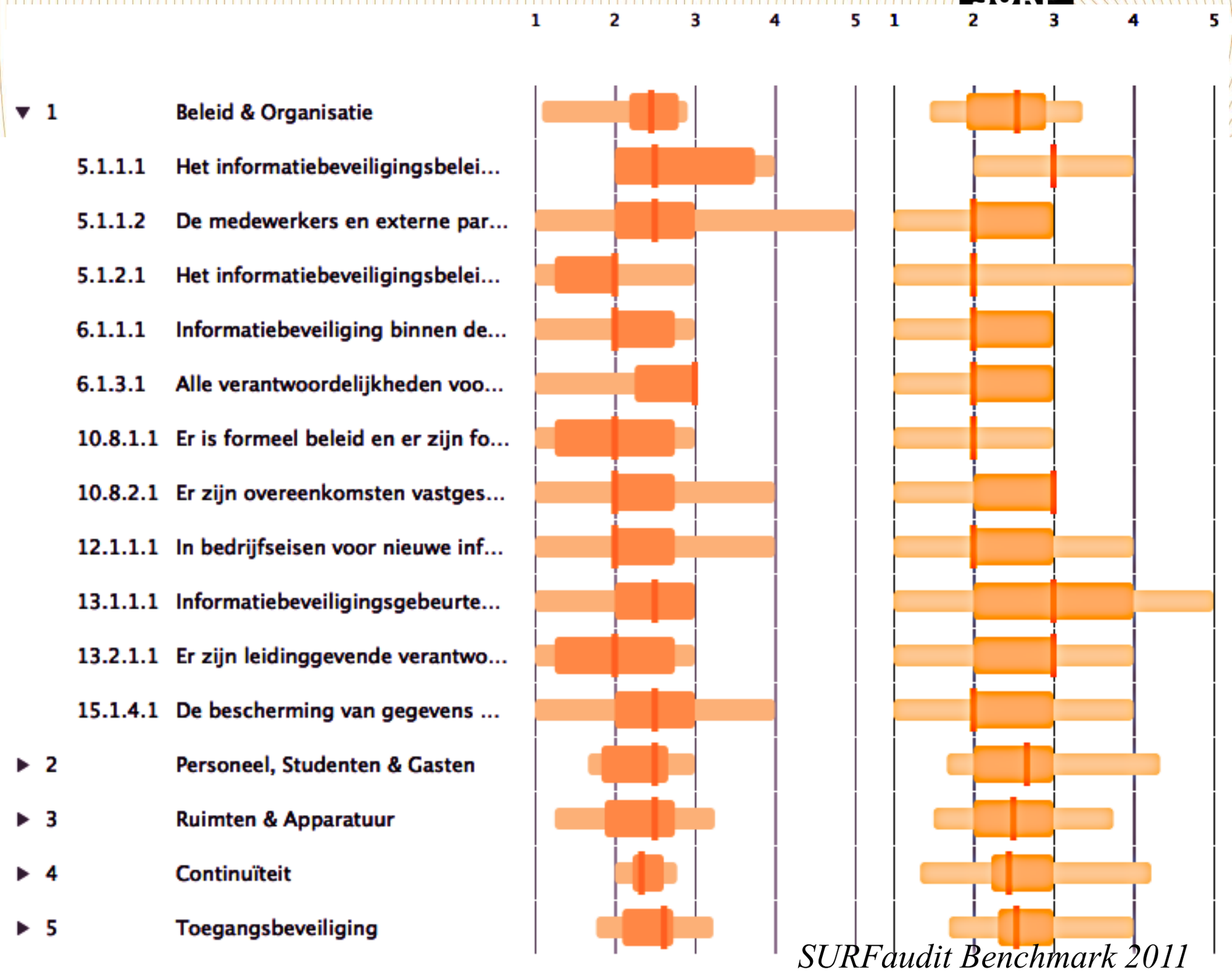
Value

CMM scoring mechanism

0	*Non-existent*	*Management processes are not applied at all.*	*Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.*
1	*Initial/Ad Hoc*	*Processes are ad hoc and disorganised.*	*There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.*
2	*Repeatable but Intuitive*	*Processes follow a regular pattern.*	*Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.*
3	*Defined Process*	*Processes are documented and communicated.*	*Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.*
4	*Managed and Measurable*	*Processes are monitored and measured.*	*Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.*
5	*Optimised*	*Good practices are followed and automated.*	*Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.*

Tabel 2: CMM scoringsmodel

SURF

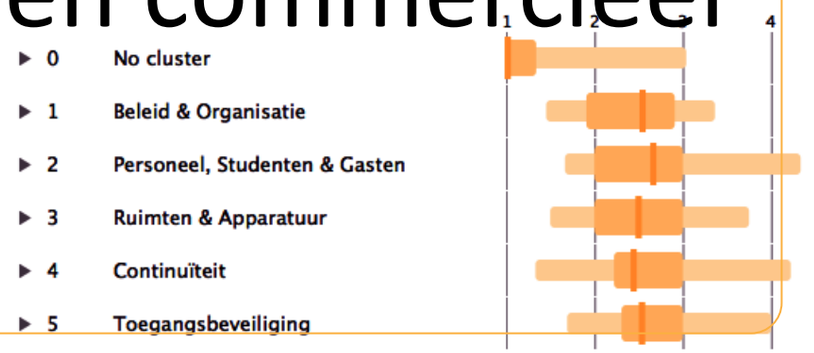


Niveau	Omschrijving
0	*Non-existent*
1	*Initial/Ad Hoc*
2	*Repeatable but Intuitive*
3	*Defined Process*
4	*Managed and Measurable*
5	*Optimised*

SURFaudit Benchmark 2011

Use and re-use

- Framework informatiebeveiliging en normenkader zijn gebaseerd op internationale standaards en de EU wetgeving: Zijn vrij becshikbaar
- Benchmark getallen zijn/wordne gepubliceerd
  - Landelijke benchmark?
- Tooling die nu gebruikt wordt is een commercieel product



FOKKE & SUKKE

SLAPEN ER NIET VAN

Project Regie in de Cloud
referentie Architectuur (HORA)
Classificatie van gegevens
Juridisch Normenkader

SIG Digitale Rechten
Kennisbank
Vraagbaak
Intellectueel eigendom

SURFacademy: Privacy Curriculum
Introductie Europese richtlijn.
Privacy impact Assessments
Privacy Beleid
Impact wetenschappelijk Onderzoek

SURFibo
Leidraden Security en Privacy
CERT/IBO Security congres

SURF: Rapporten en papers
Patriot Act en FISA
Uitspraak CBP over cloud
Persoonsgegevens in Botnets
Authenticatie voor informatiesystemen
Rechtmatig operationeel handelen

SURFnet/SURFconext
Step-up Authenticatie (as-a-service)
SURFcertificaten

WHAT SURF CAN DO

Meer weten?

Hoger Onderwijs Referentie Architectuur, HORA: http://www.wikixl.nl/wiki/hora
Framework informatiebeveiliging: http://www.surf.nl/themas/beveiliging
CBP Richtsnoer beveiliging persoonsgegevens
(http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx)

Alf Moens
alf.moens@surf.nl

WHAT SURF CAN DO