Universitair Informatiemanagement

UNIVERSITEIT TWENTE.

Kenmerk: SB/UIM/14/0902/khv
Datum: 13 maart 2015

Ambitieniveau SURFaudit

In SURF-verband is afgesproken dat de instellingen de SURFaudit uitvoeren om het niveau van de informatiebeveiliging te meten.

Zowel in 2012 en 2013 heeft de UT de SURFaudit als self-assessment uitgevoerd. Tot nu toe heeft de UT geen expliciete doelstelling ten aanzien van het gewenste volwassenheidsniveau vastgesteld.

In de SURFaudit wordt gemeten welk volwassenheidsniveau wordt behaald op een schaal van 0 (non-existent) tot 5 (optimized). Het gemiddelde van de instellingen die aan de SURF assessment hebben mee gedaan lag in de meest recente audit (2013) net boven de 2. Het resultaat van SURFaudit 2013 laat zien dat de UT gemiddeld net onder niveau 3 scoort.

De UT scoort relatief slecht op de laatste twee aspecten, het bedrijfscontinuïteitbeheer en de naleving. Hier scoort de UT op niveau 2. De grootste kwetsbaarheid wordt veroorzaakt door de aspecten met de laagste scores. Voor het bereiken van een beter resultaat is een bredere inzet nodig dan alleen van UIM en ICTS (bijvoorbeeld van systeemhouders en functioneel beheerders).

Gevraagd besluit

Het college wordt gevraagd om het belang van security en privacy voor de UT te onderstrepen door zich conform het advies van SURF uit te spreken voor een aantoonbaar volwassenheidsniveau 3 (op een schaal van 0-5) voor alle aspecten van de SURFaudit.

Achtergrondinformatie

Om het volwassenheidsniveau van de informatiebeveiliging te kunnen meten is door SURF de tool SURFaudit ontwikkeld met als doelstelling:

“SURF-audit is in eerste instantie bedoeld om instellingen individueel en gemeenschappelijk zicht te geven op de zwakke plekken, zodat daarop maatregelen kunnen worden genomen. In tweede instantie is het bedoeld om als sector onderling (voor de onderlinge IT-services) en naar de samenleving aan te kunnen tonen dat beveiliging en privacy in het HO goed en professioneel is geregeld. De eerste doelstelling halen we als instellingen vrijwillig meewerken aan self assessments en periodiek (één x per ca. vier jaar) aan een onafhankelijke toets. De tweede doelstelling halen we alleen als alle instellingen zich periodiek willen laten toetsen.”

In de audit worden de maatregelen uit een normenkader gescoord volgens een vast mechanisme. Zowel in 2012 als in 2013 heeft de UT, met ondersteuning vanuit Operational Audit (OA), de SURFaudit als self-assessment uitgevoerd. In 2015 is de UT voornemens om na een self-assessment een peer review uit te laten voeren, dat wil zeggen dat deskundigen van twee andere instellingen (een deel van) de SURFaudit van de UT beoordelen

Normenkader

In 2011 heeft SURF het eerste normenkader voor informatiebeveiliging in het Hoger Onderwijs opgesteld. Het normenkader is een selectie van de belangrijkste toetselementen van ISO 27002 en sluit goed aan bij het Informatiebeveiligingsbeleid Universiteit Twente[1], dat nadrukkelijk verwijst naar ISO 27002[2] als norm.

Het College Bescherming Persoonsgegevens (CBP) heeft in 2013 een audit informatie-beveiliging uitgevoerd bij twee hogescholen[3] en heeft de richtsnoeren Beveiliging van persoonsgegevens[4] uitgebracht. Op grond hiervan heeft SURF het normenkader uitgebreid van 40 naar 84 maatregelen.

Volwassenheidsniveau en CMM

Met SURFaudit worden de bestaande beveiligingsmaatregelen (baseline) gescoord op volwassenheidsniveau, waarbij is gekozen voor het Capability Maturity Model (CMM).

CMM zoals gehanteerd bij de SURFaudit kent de volgende volwassenheidsniveaus:[5]

0.	Non-existent	Management processes are not applied at all
1.	Initial / Ad Hoc	Processes are ad hoc and disorganised
2.	Repeatable but intuitive	Processes follow a regular pattern
3.	Defined Process	Processes are documented and communicated
4.	Managed and Measurable	Processes are monitored and measured
5.	Optimized	Good practices are followed and automated

Afweging

De UT voert (bijna) jaarlijks een SURFaudit uit op de securityaspecten van haar ICT- en informatievoorzieningen. Tot nu toe heeft de UT geen expliciete doelstelling ten aanzien van het gewenste volwassenheidsniveau vastgesteld. Voorgesteld wordt om het gewenste volwassenheidsniveau aantoonbaar op 3 (defined process) te stellen.

Niet uniform werken (niveau 2) veroorzaakt securityrisico's en minder beheersbare processen. Een score van 2 of lager op een deelaspect identificeert een verbeterpunt.

Een gedefinieerd proces (niveau 3) betekent dat er vastgesteld beleid is en dat dit middels procedures is geïmplementeerd. Verantwoordelijkheid wordt op het juiste niveau genomen en processen worden beheersbaarder. Dit wordt gezien als het minimaal noodzakelijke niveau.

Verbeteren door te meten (niveau 4) wordt gezien als nastrevenswaardig. Echter wanneer de afweging gemaakt moet worden om een deelaspect van niveau 2 naar 3 te brengen of een ander deelaspect van 3 naar 4, dan wordt het behalen van het minimumniveau van groter belang geacht. Daarom kiest de UT er vooralsnog voor om de norm op niveau 3 te stellen.

---

[1] zie http://www.utwente.nl/sb/uim/informatiebeveiliging/informatiebeveilingsbeleid_ut.pdf
[2] ISO 27002 Code voor Informatiebeveiliging
[3] zie https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2013_beveiliging-persoonsgegevens-studenten-hogeschool-arnhem-nijmegen.pdf en https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2013_beveiliging-persoonsgegevens-studenten-hogeschool-utrecht.pdf
[4] https://cbpweb.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013
[5] voor meer achtergrondinformatie zie http://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2011/SURFaudit+Inrichtingsvoorstel+2011+v1.2.pdf

Objectiviteit

Om te voorkomen dat de resultaten van de audit afhangen van de subjectieve mening van deelnemers is het van belang dat een bepaald volwassenheidsniveau ook aangetoond kan worden. Hierdoor zou een self-audit niet heel andere resultaten moeten opleveren als een externe audit.

In 2015 is de UT voornemens om na een self-assessment een peerreview uit te laten voeren, dat wil zeggen dat twee deskundigen van andere instellingen (een deel van) de SURFaudit van de UT beoordelen. Hierbij zal met name het bewijsmateriaal beoordeeld worden. In ruil zal de security officer een peerreview bij twee andere instellingen uitvoeren.

Resultaten SURFaudit 2013

Hieronder staat een samenvatting van de resultaten van het assessment 2013 van de UT en de overige deelnemende instellingen.