ROSA Architectuurscan/advies: SURF Security Baseline

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	Joeri van Es en Remco de Boer
Versie	2e concept
Datum	20/12/2023
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met de indiener en direct betrokkenen definitief: behandeld door Architectuurraad
Aanleiding	Binnen het hoger onderwijs en middelbaar beroepsonderwijs hanteerden instellingen tot voor kort hun eigen beveiligingsmaatregelen, zowel voor intern gebruik als voor eisen aan leveranciers. Door de variatie in deze maatregelen was er echter geen eenduidig kader voor leveranciers om aan te voldoen, en samenwerking tussen de instellingen was uitdagend door de verschillen.
Betreft	**SURF Security Baseline**
Brondocument(en)	[1] Achtergrond over de baseline doelen: https://communities.surf.nl/cybersecurity/artikel/surf-security-baseline-onderwijs-en-onderzoek-beschikbaar [2] Gebruikshandleiding: https://sec.surf.nl/security-baseline-achtergrond/ [3] De maatregelenset/baseline zelf: https://sec.surf.nl/controls/ [4] Aanmeldformulier SURF Security Baseline bij Edustandaard
Begeleidende documenten	

Inleiding

Met de ROSA Architectuurscan worden op systematische wijze alle architectuuraspecten van een bij Edustandaard ingebracht onderwerp in kaart gebracht en worden knelpunten en kansen gesignaleerd. Niet alleen kan de indiener er zijn voordeel mee doen, ook kan ROSA ermee worden verrijkt. En tot slot stelt het andere ketenpartijen in staat om kennis te nemen van architectuurwijzigingen en het belang hiervan voor de eigen organisatie of achterban te bepalen (transparantie in de keten, informatiepositie).

Dit formulier bevat de uitkomst van een architectuurscan van het **SURF Security Baseline**. Voor de indiener biedt de scan concrete handvatten voor toepassing van ROSA, en de mogelijkheid om lessen en ervaringen uit het project terug te koppelen aan ROSA. Een architectuurscan wordt in principe uitgevoerd met een hoge

mate van betrokkenheid van vertegenwoordigers van de inbrenger. Deze wordt hierbij ondersteund door Bureau Edustandaard, de beheerder van ROSA. De inbrenger zou zich moeten herkennen in de uitkomsten.

Iedere architectuurscan begint met de vraag: welke onderdelen van ROSA zijn relevant voor het ingebrachte onderwerp, en indien relevant, op welke wijze? Vervolgens worden de vragen gesteld hoe het ingebrachte past op wat in ROSA is uitgewerkt, en of het project wellicht inzichten heeft die kunnen leiden tot verbetering of uitbreiding van ROSA. De antwoorden op deze vragen worden verwoord in termen van een advies richting zowel inbrenger, als richting ROSA zelf. De opzet van het advies is dat per onderdeel van ROSA uitspraken worden gedaan over:

1. Bevindingen uit project: *wat zegt het project zelf over het verband met ROSA van het ingebrachte onderwerp?*
2. Relatie met ROSA: *hoe verhoudt het ingebrachte zich tot ROSA[1]?*
3. Voorgesteld advies van de Architectuurraad aan het project: *tips, verbeterpunten, en ook bekrachtiging dat er goed werk is geleverd vanuit het perspectief van ROSA[2]*
   Adviezen in deze kolom zijn, gegroepeerd in 'PRODUCT' en 'CONTEXT'. De PRODUCT-adviezen bestrijken sec het ingediende 'product', d.w.z. het **SURF Security Baseline**. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van het **SURF Security Baseline** bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen het **SURF Security Baseline** toegepast gaat worden. Deze adviezen kunnen gericht zijn aan het project zelf, maar kunnen ook zijn gericht aan partijen die zich in die context bevinden, zoals de project(deel)groep die zich richt op de implementatie van de uiteindelijke **SURF Security Baseline**, maar ook (sector)organisaties die met de uiteindelijke implementatie te maken gaan krijgen.
4. **Voorgesteld advies voor de Architectuurraad voor plaatsing onderwerpen op de ROSA architectuur backlo**g: *wat kan ROSA doen om in het vervolg een betere ondersteuning te bieden aan dit project, en andere?*

Samenhang met andere formulieren:

- **Pitch Architectuurscan**: Het doel van de architectuurpitch is om een eerste indruk te krijgen van een ketenafspraak . Op basis van de pitch en de aangeleverde documentatie voert Bureau Edustandaard een architectuurscan uit. Voor de leden van de Architectuurraad (en andere geïnteresseerden) verduidelijkt deze pitch de context van de afspraak en de resultaten uit de architectuurscan.
- **ROSA architectuurscan *bevindingen***: aan het invullen van het adviesdeel van een architectuurscan (dit formulier) gaat het verzamelen van feitelijke informatie, en het analyseren daarvan, vooraf. Die informatie, en de analyses, worden vastgelegd in het bevindingendeel van de architectuurscan. De lezer van het adviesdeel kan die erop na slaan als hij wil weten hoe het advies tot stand is gekomen. Het lezen van het bevindingendeel is niet vereist om het adviesdeel te begrijpen. Waar van toepassingen verwijst het bevindingendeel naar specifieke locaties van de brondocumenten die als input dienden voor de architectuurscan. Ook het lezen van de brondocumenten is niet vereist om het adviesdeel te begrijpen.

[1] De verhouding tussen het ingediende en de ROSA wordt per onderdeel uitgedrukt in een 'level of conformance' ontleend aan TOGAF, zie de bijlage.
[2] Dit is een concept advies, de uitkomsten worden eerst door de Architectuurraad besproken.

ROSA Architectuurscan/advies: SURF Security Baseline

ROSA-onderdeel	Bevindingen uit project: SURF Security Baseline	Relatie met ROSA (blauw: ROSA, geel: SURF Security Baseline)	Voorgesteld advies aan project	Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkingsgebied	"De SURF Security Baseline is ontworpen door en voor onderwijsinstellingen die lid zijn van SURF, waaronder universiteiten (wo), hogescholen (hbo) en middelbare beroepsscholen (mbo)." (Aanmeldformulier Edustandaard)	 **Compliant** - De SURF Security baseline is van toepassing op de werkingsgebieden bve en ho.	**PRODUCT:** **CONTEXT:**	
Ketendomeinen en -processen	De SURF Security Baseline bevat een aantal uniforme beveiligingsmaatregelen voorschrijft en zodoende bijdraagt aan een coherent beveiligingslandschap van onderwijsorganisaties binnen het HO en MBO. Informatiebeveiliging is een fundamenteel aspect dat door alle lagen van de onderwijsinformatievoorziening heen speelt.	 **Fully conformant –** Op basis van het gestelde in het aanmeldformulier van de SURF Security Baseline, kan gesteld worden dat de SURF Security Baseline raakvlakken heeft met alle ketendomeinen en -processen binnen ROSA.	**PRODUCT:** **CONTEXT:**	
Scenario	De SURF Security Baseline presenteert een samenstel van maatregelen (controls) gericht op het waarborgen van informatiebeveiliging binnen onderwijsinstellingen. Deze maatregelen zijn ontworpen om zowel nieuwe als bestaande systemen en toepassingen van de SURF-leden (onderwijsinstellingen) te laten voldoen aan een vastgesteld minimumniveau van beveiliging. [4]	 **Compliant** - Er is een relatie met het ROSA Ondersteuningsscenario Inrichten IBP-maatregelen . De SURF Security Baseline, met zijn focus op informatiebeveiliging binnen onderwijsinstellingen, sluit aan bij het ROSA-	**PRODUCT:** **CONTEXT:**	

		ondersteuningsscenario voor het inrichten van IBP-maatregelen. Deze afspraak met maatregelen ondersteunt de ketengerichte benadering van ROSA voor informatiebeveiliging en privacy, waarbij onderwijsinstellingen worden aangemoedigd hun interne beveilingsmaatregelen af te stemmen met de keten.		
Ontwerpgebied **Governance**	Bij de ontwikkeling van de SURF Security Baseline waren verschillende SURF-leden en partners betrokken, zoals vastgesteld in april 2023 [4]. Ook staat er een lijst van instellingen die hebben deelgenomen aan het opstellen van de richtlijnen op de SURF website. [1] In 2.8 van het aanmeldformulier wordt de samenhang met andere afspraken beschreven. De maatregelen lijken met name gebaseerd te zijn op internationale afspraken zoals de CIS en ISO 27001 en 27002. De relatie met het toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA wordt erkend, maar niet gespecificeerd. [4] De doelgroep werd regelmatig geïnformeerd over de baseline via bijeenkomsten van SURF-community's SCIPR en SCIRT, mailings, websites en door collega's die gespecialiseerd zijn in informatiebeveiliging. Er zijn echter geen openbare verslagen of besluitenlijsten die een brede	 **Onbepaald** - **Onbepaald met** Alle belangen in kaart**:** De betrokkenheid van verschillende SURF-leden en partners suggereert dat er inspanningen zijn gedaan om verschillende belangen in kaart te brengen, hoewel dit wellicht verder uitgewerkt kan worden voor een volledig overzicht. **Onbepaald met** Bewaak relaties met andere afspraken: Het is onduidelijk hoe de SURF Security Baseline zich verhoudt tot het toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA en de Uniforme Beveiligingsvoorschriften en of er afstemming met deze afspraken is georganiseerd. Ook is onduidelijk hoe deze	**PRODUCT:** • Versterk de inspanningen om alle relevante belangen in kaart te brengen. Dit kan door een meer gestructureerde stakeholderanalyse uit te voeren waarbij alle betrokken partijen en hun belangen expliciet worden geïdentificeerd en gedocumenteerd. • Ontwikkel een governance mechanisme voor het afstemmen van de SURF Security Baseline met gerelateerde afspraken, zoals het toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA. • Voer een gedetailleerde analyse uit waarbij per maatregel van de	

	acceptatie van de afspraak aantonen. [4]	afhankelijkheden traceerbaar worden gemaakt. **Compliant met** Transparantie over deelname: Het is duidelijk wie aan ontwikkeling van de afspraak hebben deelgenomen.	SURF Security Baseline de relaties met andere relevante afspraken in het onderwijsdomein in kaart worden gebracht. • Positioneer de SURF Security baseline ten opzichte van het ROSA certificeringsschema. • Maak de afhankelijkheden met andere afspraken traceerbaar op het niveau van individuele maatregelen. **CONTEXT:**	
Ontwerpgebied **IBP**	Aangezien de maatregelen in de SURF Security Baseline zijn gerelateerd aan de maatregelen uit het toetsingskader van het certificeringsschema, kon een globale verschillenanalyse worden uitgevoerd. [4] De belangrijkste verschillen op een rij: • Classificatie: ROSA hanteert de BIV-methodiek, terwijl SURF werkt met securitylevels. Dit resulteert in een verschillende benadering van risicoclassificatie. Hoewel de controls in de baseline risicoschaling aangeven, is het niet altijd duidelijk wat de criteria zijn voor het classificeren van applicaties als 'medium' en 'high'. [3] • Categorieën: ROSA gebruikt 21 categorieën,	**Explain -** **Explain met** Hanteer Certificeringsschema ROSA en Gebruik UBV: De SURF Security Baseline hanteert een andere aanpak in classificatie, categorieën, en maatregelen dan het Certificeringsschema ROSA, wat leidt tot verschillen in de uitvoering van informatiebeveiligingsbeleid.	**PRODUCT:** • Harmoniseer de classificatie- en maatregelmethoden van de SURF Security Baseline met die van ROSA voor een uniforme benadering van informatiebeveiliging. • Het is raadzaam een gedetailleerde uitleg of handreiking op te stellen die de criteria voor de risicoanalyse en classificatie van applicaties in 'medium' en 'high' uiteenzet. **CONTEXT:** • Het is ook raadzaam om het ROSA Certificeringsschema te	Het is geobserveerd dat het ROSA Certificeringsschema binnen het Hoger Onderwijs momenteel beperkt wordt toegepast, ondanks een overlappend werkingsgebied. De AR wordt geadviseerd een analyse uit te voeren om de onderliggende redenen voor deze beperkte implementatie te identificeren.

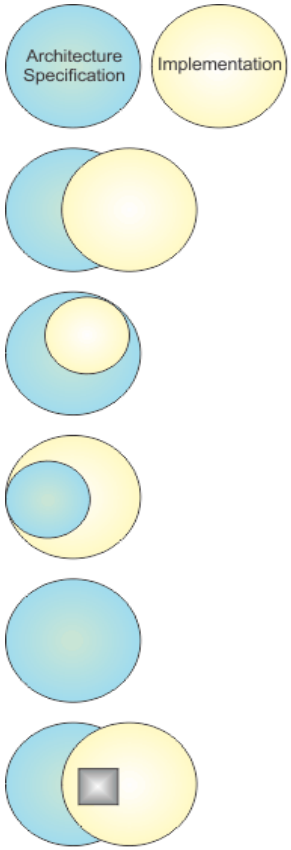
	terwijl SURF er 18 heeft. De indeling en het aantal categorieën variëren. [3] • Maatregelen: ROSA heeft meerdere, ongemarkeerde maatregelen per categorie, in tegenstelling tot de duidelijk gemarkeerde maatregelen in SURF. [3] • Scope: De scope van ROSA is meer technisch en procesmatig, terwijl SURF een bredere scope heeft, inclusief organisatorische maatregelen. • Taal: Een taalverschil bestaat; ROSA is in het Nederlands en SURF in het Engels.		herzien in het licht van deze harmonisatie. • Overweeg de integratie van SURF's bredere organisatorische focus in de normenkaders voor Informatiebeveiliging en Privacy binnen onderwijsinstellingen.	
Ontwerpgebied **Interoperabiliteit**		**Irrelevant –** Er is geen overlap tussen ontwerpkaders uit de ROSA en inhoud van Security Baseline maatregelen.	**PRODUCT:** **CONTEXT:**	
Ontwerpgebied **IAA**	De afspraak zelf is openbaar toegankelijk. Hier is geen IAA voor nodig. Wel gaan een 13 van de maatregelen over dit onderwerp. **SB.9.013 Digital Identities:** Garandeert dat digitale accounts en identificatoren altijd uniek gekoppeld zijn aan een natuurlijk persoon en dat oude accounts en unieke accountinformatie nooit opnieuw worden toegewezen aan andere natuurlijke personen. Dit waarborgt	**Compliant** - **Compliant met** Een persoon heeft minstens één digitale identiteit en Sturing op gebruik van digitale identiteit: implementatie van maatregel SB.9.013 zorgt ervoor dat digitale identiteiten traceerbaar en controleerbaar	**PRODUCT:** **CONTEXT:**	

	de traceerbaarheid van digitale toegang tot een unieke individu. **SB.9.015 Joiner/Mover/Leaver:** Vereist dat proceseigenaren goedkeuring verlenen aan gebruikers die autorisaties ontvangen voor gegevens binnen het proces. Dit omvat het loggen en bewaren van verzoeken om toegang tot informatie-assets en bijbehorende autorisaties, alsmede het documenteren van intrekkingsverzoeken en wijzigingen in rollen of contractuele relaties. **SB.9.016 Authorization Matrix:** Legt de verantwoordelijkheid bij proceseigenaren voor een autorisatiematrix die vastlegt wie toegang heeft tot welke gegevens en in welke hoedanigheid. De matrix omvat rollen, autorisaties in rollen, individuen en de rollen die aan individuen zijn toegestaan.	blijven, in overeenstemming met de ROSA-ontwerpkaders over dit onderwerp. **Compliant met** Maak uitvoering transparant: Door het loggen en documenteren van toegangs- en autorisatieverzoeken, evenals wijzigingen in rollen en contractuele relaties, wordt de transparantie voor de betrokken personen verhoogd. **Compliant met** Maak in ontwerp (van vertrouwensraamwerk) transparant hoe privacy is geborgd: De maatregel SB.9.016 voldoet aan het ROSA ontwerpkader door expliciet de toegangsrechten en rollen binnen de organisatie te definiëren, wat bijdraagt aan duidelijke privacyborging en informatiebeveiliging in het ontwerp.		
Ontwerpgebied **M2M Interactie**		**Onbepaald** – Dit ontwerpgebied is nog niet uitgewerkt in de ROSA.	**PRODUCT:** **CONTEXT:**	

Ontwerpgebied **H2M Interactie**		**Onbepaald** - Dit ontwerpgebied is nog niet uitgewerkt in de ROSA.	**PRODUCT:** **CONTEXT:**	
Referentie-componenten en ketenvoorzieningen	De SURF Security Baseline bevat diverse maatregelen gericht op het verhogen van de beveiliging van informatiesystemen binnen onderwijsinstellingen.Binnen deze maatregelen zijn uitspraken opgenomen over 'assets', een term die binnen de context van informatiebeveiliging breed geïnterpreteerd kan worden. Dit omvat alle vormen van applicaties, zowel hardware als software. Een specifieke maatregel, SB.1.004 'Asset inventory', benadrukt het belang van het bijhouden van een actuele inventarisatie van alle hardware- en software-assets binnen een organisatie. [3]	**Onbepaald** – Al lijken er geen specifieke ketenvoorzieninngen en RC's betrokken te zijn bij implementatie van deze afspraak, gezien de definitie van 'assets' in de maatregelen, heeft deze een relatie met het referentiecomponent: **Gegevensverwerkend Systeem** Aan dit referentiecomponent is het ROSA ontwerpkader gekoppeld: **Hanteer Certificeringsschema ROSA.** Echter, de mate waarin de implementatie van de SURF Security Baseline ook de vereisten van het ROSA certificeringsschema invult, blijft onbepaald.	**PRODUCT:** **CONTEXT:**	Faciliteer een afstemming tussen het certificeringsschema van ROSA en de SURF Security Baseline met als doel: onderzoek en documenteer hoe de implementatie van de SURF Security Baseline kan bijdragen aan het voldoen aan het ROSA certificeringsschema.
Beheer en (door)ont-wikkeling	Het beheer en de doorontwikkeling van de SURF Security Baseline zijn gestructureerd via twee primaire organen: het 'standaard committee' en de 'regiegroep'. [4] Daarnaast is er een proces van aankondiging en feedback voor geplande wijzigingen. Dit proces zorgt ervoor dat alle leden van		**PRODUCT:** Overweeg het instellen van een formeel proces (geïnspireerd door BOMOS) voor de continue beoordeling en bijwerking van de baseline, rekening houdend met ontwikkelingen binnen gerelateerde afspraken aan de Security Baseline, zoals de ISO	

	SURF, vertegenwoordigd in verschillende gremia, geïnformeerd zijn over voorgestelde wijzigingen en de gelegenheid hebben om feedback te geven. Tot slot is de Raad van Bestuur (RvB) van SURF verantwoordelijk voor het nemen van het uiteindelijke besluit over de vaststelling van de baseline. Er is geen intentie of behoefte om de baseline onder te brengen bij een werkgroep binnen Edustandaard.		27000 standaarden en gerelateerde Edustandaard afspraken. **CONTEXT:**	
Implementatie			**PRODUCT:** **CONTEXT:**	

Bijlage 1: **ARCHITECTURE COMPLIANCE (TOGAF)**



Irrelevant:
The implementation has no features in common with the architecture specification (so the question of conformance does not arise).

Consistent:
The implementation has some features in common with the architecture specification, and those common features are implemented in accordance with the specification. However, some features in the architecture specification are not implemented, and the implementation has other features that are not covered by the specification.

Compliant:
Some features in the architecture specification are not implemented, but all features implemented are covered by the specification, and in accordance with it.

Conformant:
All the features in the architecture specification are implemented in accordance with the specification, but some more features are implemented that are not in accordance with it.

Fully Conformant:
There is full correspondence between architecture specification and implementation. All specified features are implemented in accordance with the specification, and there are no features implemented that are not covered by the specification.

Non-conformant:
Any of the above in which some features in the architecture specification are implemented not in accordance with the specification.

Bron: http://pubs.opengroup.org/architecture/togaf9-doc/arch/Figures/48_conformance.png

Een Nederlandse vertaling van de beschrijving van de TOGAF-categorieen:

a. **irrelevant** = er is geen relatie tussen het ingebrachte en ROSA
b. **consistent** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is het ingebrachte conform ROSA gerealiseerd, de overlap is echter niet **volledig** = sommige specificaties van ROSA zijn niet overgenomen, en het ingebrachte heeft onderdelen die niet door ROSA worden gedekt.
c. **compliant** = het ingebrachte valt volledig binnen ROSA (subset) en is conform ROSA gerealiseerd
d. **conformant** = ROSA dekt alleen een deel van het ingebrachte, maar dat deel is wel conform ROSA gerealiseerd
e. **fully conformant** = ROSA dekt het geheel van het ingebrachte, en niets van het ingebrachte valt buiten ROSA
f. **non-conformant** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is er iets van het ingebrachte *niet* conform ROSA gerealiseerd