



Statement

ISAE3402

Information Security, Privacy & Compliance

Als serviceorganisatie erkennen we het belang van beheersmaatregelen die we als onderdeel van en ter ondersteuning van onze aangeboden diensten hebben ontwikkeld, geïmplementeerd en uitgevoerd. Daarom laten wij een ISAE3402-rapport opstellen door een onafhankelijke auditor. Het ISAE3402-rapport behandelt de interne beheersmaatregelen van systemen binnen de scope van de rapportage. Deze beheersmaatregelen zijn relevant voor klanten die gebruik maken van deze systemen. Klanten kunnen de ISAE3402-rapportage gebruiken voor hun interne controle met betrekking tot de jaarrekening.

Exact MKB Software B.V. heeft een ISAE3402-rapportage voor datacenterhosting en clouddiensten. De rapportage, de beschrijving van toetsing en van interne beheersingsmaatregelen zijn alleen beschikbaar voor bestaande klanten of voor auditoren van bestaande klanten. Mocht u niet onder deze groep vallen, dan is dit statement voor u opgesteld.

Scope van de rapportage

Exact MKB Software B.V. heeft de volgende scope gedefinieerd voor de ISAE3402-rapportage:

“Het ontwerp, de implementatie en de werking van datacenterhostingservices, inclusief de levering van beheerde services, ondersteuning en clouddiensten.”

Diensten die vallen binnen deze scope worden vanuit de volgende locaties aangeboden, waarbij gebruik wordt gemaakt van onafhankelijke datacenters van derden of onafhankelijke Public Cloud providers:

- Digital Realty, Amsterdam, The Netherlands.
- BIT, Ede, The Netherlands
- Azure, EU data centers

Vanuit het kantoor in Utrecht ontwikkelt en beheert Exact MKB Software, die in 2020 nog handelde onder de naam “Unit4 Bedrijfssoftware” de SaaS en Clouddiensten. Aangeboden diensten zijn:

- Accountancy Software as a Services
- Boekhoud Gemak / Multivers (vanaf okt. 2020)
- Personeel&Salaris as a Services (HR&Salaris Gemak - SalarisCloud)
- Smart Desktop services
- Back-up and Restore Services
- Private Servers
- Connectivity services
- Managed services

Rechten

Aan dit statement kunnen geen rechten worden ontleend.

Gedefinieerde beheerdoelstellingen

Exact MKB Software B.V. heeft onderstaande beheerdoelstellingen gedefinieerd die zijn onderzocht door een externe onafhankelijke auditor. Deze beheerdoelstellingen zijn gekoppeld aan Trust Services Criteria en COSO model

Gedefinieerde Beheersdoelstelling	TSC-#	TSC-Verwijzing
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat commitment aan ethiek en integriteit wordt uitgedragen	1.1	COSO Principle 1
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat er een effectieve Information Security Risk Board is	1.2	COSO Principle 2
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat management structuren en reporting lines heeft geïmplementeerd	1.3	COSO Principle 3
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de juiste informatie beschikbaar is voor het uitvoeren van de interne controle functie	2.1	COSO Principle 13
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat interne communicatie over interne beheersing plaatsvindt	2.2	COSO Principle 14
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de effectiviteit van interne controle wordt geëvalueerd	4.1	COSO Principle 16
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de doelstellingen ten aanzien van risico identificatie en assessment voldoende specifiek zijn	3.1	COSO Principle 6
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat risico's worden geïdentificeerd en worden gewogen	3.2	COSO Principle 7
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de risico beperkende activiteiten risico's tot een acceptabel niveau terugbrengen	5.1	COSO Principle 10
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat er richtlijnen zijn voor risico mitigatie die ook geïmplementeerd zijn	5.3	COSO Principle 12
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat tekortkomingen in de interne beheersing tijdig worden gecommuniceerd en verholpen	4.2	COSO Principle 17
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de entiteit zich inspant om competente medewerkers aan te stellen, te ontwikkelen en te behouden	1.4	COSO Principle 4
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat individuen verantwoordelijk worden gehouden voor hun bijdrage aan interne beheersing	1.5	COSO Principle 5
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat fraude in voldoende mate wordt meegenomen in de risico analyses	3.3	COSO Principle 8
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat wijzigingen in de organisatie worden meegenomen in de risk assessments	3.4	COSO Principle 9

Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie logische toegangsbeveiliging heeft geïmplementeerd binnen de software, infrastructuur en architectuur van informatiemiddelen.	6.1	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat gebruikers worden geregistreerd en geautoriseerd alvorens zij inloggegevens tot hun beschikking krijgen en dat deze inloggegevens worden ingetrokken op het moment dat een gebruiker niet langer geautoriseerd is.	6.2	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot data, software, functies en andere informatiemiddelen wordt geautoriseerd, aangepast en verwijderd op basis van rollen, verantwoordelijkheden of het ontwerp van het systeem en wijzigingen, hierbij wordt uitgegaan van de principes van "need to know" en functiescheiding.	6.3	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie fysieke toegang tot gebouwen en informatiemiddelen beperkt tot geautoriseerd personeel.	6.4	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie wijzigingen op een beheerste manier doorvoert.	8.1	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie de vraag naar capaciteit beheerst en aanvullende capaciteit inzet indien nodig.	10.1	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat beveiligingsincidenten worden geëvalueerd om vast te stellen in hoeverre deze invloed kunnen hebben, of hebben gehad, op de doelstellingen van de organisatie, en dat er actie wordt ondernomen om deze invloed te voorkomen of te adresseren.	7.3	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie reageert op de geïdentificeerde beveiligingsincidenten conform een formeel proces om incidenten te begrijpen, in te perken, te verhelpen en te communiceren indien nodig.	7.4	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie vertrouwelijke informatie identificeert en onderhoudt om zo haar doelstellingen met betrekking tot vertrouwelijkheid te behalen.	11.1	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie zich ontdoet van vertrouwelijke informatie op een manier om zo haar doelstellingen met betrekking tot vertrouwelijkheid te behalen.	11.2	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de logische en fysieke toegangsbeveiliging van fysieke middelen pas worden opgeheven wanneer deze niet meer binnen de beheersingsfeer van de organisatie vallen	6.5	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie de verzending, verplaatsing en verwijdering van informatie beperkt tot geautoriseerde interne en externe gebruikers en processen, en dat de informatie beschermd wordt tijdens verzending, verplaatsing of verwijdering.	6.7	Criteria Outside of the COSO Principles

Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie in staat is om te herstellen van geïdentificeerde beveiligingsincidenten.	7.5	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie mogelijke risico's op verstoering van de bedrijfsvoering identificeert en mitigeert.	9.1	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie beschermd is tegen omgevingsfactoren en de software, data en infrastructuur kan herstellen indien nodig.	10.2	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de door de organisatie gedefinieerde herstel plannen en procedures getest worden.	10.3	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat voldoende gebruik wordt gemaakt van techniek bij het terugbrengen van risico's	5.2	COSO Principle 11
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat het inbrengen van ongeautoriseerde of kwaadaardige software wordt voorkomen of gedetecteerd en geadresseerd.	6.8	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de informatiesystemen van de organisatie zijn beschermd tegen bedreigingen van buiten de grenzen van deze systemen.	6.6	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie wijzigingen aan configuraties die resulteren in nieuwe kwetsbaarheden en vatbaarheid voor nieuw geïdentificeerde kwetsbaarheden detecteert en monitort.	7.1	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat afwijkingen in systeem componenten en de werking van die componenten worden gedetecteerd en geanalyseerd.	7.2	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de organisatie risico's die voortvloeien uit het gebruik van producten en diensten van derden evalueert en beheerst. bieden een redelijke mate van zekerheid dat de organisatie risico's die voortvloeien uit het gebruik van producten en diensten van derden evalueert en beheerst.	9.2	Criteria Outside of the COSO Principles
Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat afstemming met externe partijen plaatsvindt over interne beheersing	2.3	COSO Principle 15

ISAE3402 TYPE II ASSURANCE RAPPORT

Unit4 Bedrijfssoftware

Het ontwerp, de implementatie en de werking van
datacenterhostingservices, inclusief de levering van beheerde
services, ondersteuning en clouddiensten over de verslagperiode 1
januari 2020 tot en met 31 december 2020.



Doel rapportage en onafhankelijke auditor:



1.7 Beoogde gebruikers en doel

Deze rapportage en de beschrijving van toetsingen van interne beheersingsmaatregelen zijn alleen voor klanten die gebruik hebben gemaakt van het systeem van Unit4 Bedrijfssoftware en hun service auditors, die voldoende inzicht hebben om het in aanmerking te nemen bij het inschatten van de risico's op afwijkingen van materieel belang in de financiële overzichten van klanten, tezamen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door klanten zelf worden uitgevoerd.

Dit rapport mag uitsluitend in zijn geheel worden gedeeld met bovengenoemde klanten en hun service auditors. Het is niet toegestaan om delen van het rapport te verspreiden in welke vorm dan ook (elektronisch, papier of anderszins) of delen te gebruiken voor andere doeleinden dan hierboven benoemd.

