4CEE

ICREATIVE PART OF 4CEE

EASY SYSTEMS PART OF 4CEE

STIPLY PART OF 4CEE

COFORCE PART OF 4CEE

TRADE INTEROP PART OF 4CEE

DIESIS PART OF 4CEE

# Statement of Applicability ISO/IEC 27001:2022 & ISO/IEC 27017:2015

| | |
|---|---|
| Date: | January 6, 2025 |
| Version: | 2025.1.1 |
| Classification: | Public |

## 1. Introduction

This document includes the Statement of Applicability associated with the Certification for ISO 27001 and ISO/IEC 27017:2015.

The purpose of this document is to determine which control measures have been selected and the reasoning for this.

## 2. Scope

The full scope of application of 4CEE B.V. (ISO 27001, 27017 and ISO 9001):

"**Supporting the companies within the group with services in the field of management, housing, facilities, IT, HRM, finance, and marketing.**"

The full scope of ICreative B.V. (ISO 27001, 27017 and ISO 9001):

**"Advising, developing, implementing, hosting and managing software for administrative and financial processes"**

The full scope of application of Easy Systems B.V. (ISO 27001, 27017 and ISO 9001):

**"Advising, developing, implementing, hosting and managing software for administrative and financial processes"**

The full scope of Diesis Consultancy B.V. (ISO 27001, 27017 and ISO 9001):

**"Advising, developing, implementing, hosting and managing software for administrative and financial processes"**

The full scope of application of Stiply B.V. (ISO 27001, 27017 and ISO 9001):

**"Advising, developing, implementing, hosting and managing software for administrative and financial processes"**

The full scope of application of Quintensis B.V. (ISO 27001):

**"Advising, developing, implementing, hosting and managing software for administrative and financial processes"**

## 4. Applicability matrix

| A. 5 | Organisational Controls | Selected Yes / No | | If selected, reason for inclusion | Implemented Yes / No | If not selected, reason for exclusion |
|---|---|---|---|---|---|---|
| | | ISO 27001 :2022 | ISO 27017 :2015 | | | |
| A.5.1 | Policies for information security | Yes | Yes<br>5.1.1<br>CSC<br>CSP<br>5.1.2 | - Clear guidelines: Ensuring consistent and transparent guidelines to secure information.<br>- Provide framework: Helps establish a structured framework for information security. | Yes | |
| A.5.2 | Information security roles and responsibilities | Yes | Yes<br>6.1.1<br>CSC<br>CSP | - Establish responsibilities: Ensure that everyone understands their role in information security.<br>- Increased Accountability: Ensures that specific individuals are accountable for security measures. | Yes | |
| A.5.3 | Segregation of duties | Yes | Yes<br>6.1.2 | - Risk management: Prevents conflicts of interest and errors by separating responsibilities.<br>- Fraud prevention: Reduces the likelihood of fraudulent activity within an organization. | Yes | |
| A.5.4 | Management responsibilities | Yes | Yes<br>7.2.1 | - Top-down support: Management involvement ensures compliance with security policies and procedures.<br>- Direction: Provides clear direction and priorities in information security initiatives. | Yes | |
| A.5.5 | Contact with authorities | Yes | Yes<br>6.1.3 | - Compliance: Ensures that the organization meets legal and | Yes | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  |  | CSC<br>CSP | regulatory requirements.<br>- Cooperation: Facilitates cooperation with government agencies in the event of security incidents (e.g. contact with the fire brigade) and services whose characteristics are regulated by law (e.g. contact with NPA and the Tax and Customs Administration about Peppol and Vida). |  |  |
| A.5.6 | Contact with special interest groups | Yes | Yes<br>6.1.4 | - Knowledge sharing: Access to information and resources that can help improve information security practices.<br>- Networking: Provides opportunities to network with peers and experts.<br>Examples, E-invoicing standards & software | Yes |  |
| A.5.7 | Threat intelligence | Yes | Not in norm | - Proactive protection: Helps identify and analyze potential threats before they manifest.<br>- Staying up-to-date: Ensures that the organization is aware of the latest threats and vulnerabilities.<br>Risk management: RA-2021-0001 | Yes |  |
| A.5.8 | Information security in project management | Yes | Yes<br>6.1.5<br>14.1.1<br>CSC<br>CSP | - Integration: Ensures that security measures are integrated into project plans from the start. Professional services are an important part of our business | Yes |  |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | In accordance with customer agreement | | |
| A.5.9 | Inventory of information and other associated assets | Yes | Yes<br>8.1.1<br>CSC<br>CSP<br>8.1.2 | - Resource Management: Helps manage and protect all information and related assets. - Overview: Provides a complete overview of what needs to be protected. | Yes | |
| A.5.10 | Acceptable use of information and other associated assets | Yes | Yes<br>8.1.3<br>8.2.3 | - Mitigation of misuse: Provides clarity on what is and is not acceptable when using company resources. - Security: Contributes to the overall security of information and systems<br>Risk management: RA-2021-0026 & RA-2021-0027 | Yes | |
| A.5.11 | Return of assets | Yes | Yes<br>8.1.4 | - Post-employment security: Ensures that all assets are returned upon termination of employment, preventing unauthorized access.<br>- Control: Maintains control over where all company assets are and who has had access to them. | Yes | |
| A.5.12 | Classification of information | Yes | Yes<br>8.2.1 | - Prioritization: Helps determine the level of protection required for different types of information.<br>- Protection: Ensures that sensitive information is adequately protected (especially with the available resources, including via Intune) | Yes | |
| A.5.13 | Labelling of information | Yes | Yes | - Clarity: Makes it clear what | Yes | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  |  | 8.2.2<br>CSC | classification information has, which helps with the correct handling of it.<br>- Consistency: Ensures consistent handling and security of information. |  |  |
| A.5.14 | Information transfer | Yes | Yes<br>12.2.1<br>13.2.2<br>13.2.3 | - Safe transport: Ensures that information is transferred securely, both inside and outside the organization.<br>- Protection: Prevents interception or loss of sensitive information in transit. | Yes |  |
| A.5.15 | Access control | Yes | Yes<br>9.1.1<br>9.1.2<br>CSC | Controlled access to corporate resources based on individual privileges. Required for various laws and regulations, such as: GDPR, Data Breach Notification Act (Wet Meldplicht Datalekken), Wbni and NiS2. | Yes |  |
| A.5.16 | Identity management | Yes | Yes<br>9.2.1 | Controlled access to corporate resources based on individual privileges | Yes |  |
| A.5.17 | Authentication information | Yes | Yes<br>9.2.4<br>CSC<br>CSP<br>9.3.1<br>9.4.3 | Controlled access to corporate resources based on individual privileges | Yes |  |
| A.5.18 | Access rights | Yes | Yes<br>9.2.2<br>9.2.5 | Risk management: RA-2021-0009 & RA-2021-0030 | Yes |  |
| A.5.19 | Information security in supplier relationships | Yes | Yes<br>15.1.1<br>CSC | Risk management: RA-2021-0045<br>Underlying importance for laws and regulations such as: GDPR, | Yes |  |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Data Breach Notification Act (Wet Meldplicht Datalekken), Wbni, DORA and NiS2. | | |
| A.5.20 | Addressing information security within supplier agreements | Yes | Yes<br>15.1.2<br>CSC<br>CSP | Risk management: RA-2021-0031 | Yes | |
| A.5.21 | Managing information security in the ICT supply chain | Yes | Yes<br>15.1.3<br>CSP | Ensuring information security where it is not under your own management | Yes | |
| A.5.22 | Monitoring, review and change management of supplier services | Yes | Yes<br>15.2.1<br>15.2.2 | Risk management: RA-2021-0032, RA-2021-0037, RA-2021-0038, and RA-2021-0039 | Yes | |
| A.5.23 | Information security for use of cloud services | Yes | Not in norm | Risk management: RA-2021-0044<br>Ensuring information security where it is not under your own management | Yes | |
| A.5.24 | Information security incident management planning and preparation | Yes | Yes<br>16.1.1<br>CSC<br>CSP | Ensuring continuity of service<br>Legislation: Data Breach Notification Act (Wet Meldplicht Datalekken). | Yes | |
| A.5.25 | Assessment and decision on information security events | Yes | Yes<br>16.1.4 | Ensuring continuity of service | Yes | |
| A.5.26 | Response to information security incidents | Yes | Yes<br>16.1.5 | Ensuring continuity of service<br>Legislation: Data Breach Notification Act (Wet Meldplicht Datalekken). | Yes | |
| A.5.27 | Learning from information security incidents | Yes | Yes<br>16.1.6 | Continuous improvement of information security<br>Legislation: Data Breach Notification Act (Wet Meldplicht Datalekken), GDPR, Wbni and NIS2. | Yes | |
| A.5.28 | Collection of evidence | Yes | Yes<br>16.1.7<br>CSC | Continuous improvement of information security | Yes | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  |  |  | Legislation: Data Breach Notification Act (Wet Meldplicht Datalekken), GDPR, Wbni and NIS2. |  |  |
| A.5.29 | Information security during disruption | Yes | Yes<br>17.1.1<br>17.1.2<br>17.1.3 | Guaranteeing continuity and security of services | Yes |  |
| A.5.30 | ICT readiness for business continuity | Yes | Not in norm | Risk management: RA-2021-0043<br>Continuous improvement of information security | Yes |  |
| A.5.31 | Identification of legal, statutory, regulatory and contractual requirements | Yes | Yes<br>18.1.1<br>CSC<br>CSP<br>18.1.5<br>CSC<br>CSP | Demonstrably meeting all set requirements<br>Legislation: Data Breach Notification Act (Wet Meldplicht Datalekken), GDPR, Wbni and NIS2.<br>Risk management: RA-2022-0007 | Yes |  |
| A.5.32 | Intellectual property rights | Yes | Yes<br>18.1.2<br>CSC<br>CSP | Comply with legal requirements and guarantee services<br>Legislation: Copyright Act | Yes |  |
| A.5.33 | Protection of records | Yes | Yes<br>18.1.3<br>CSC<br>CSP | Meeting legal requirements and customer expectations | Yes |  |
| A.5.34 | Privacy and protection of PII | Yes | Yes<br>18.1.4 | Meeting legal requirements and customer expectations<br>Legislation: GDPR<br>Risk management: RA-2021-0069 | Yes |  |
| A.5.35 | Independent review of information security | Yes | Yes<br>18.2.1<br>CSC<br>CSP | Use of external knowledge to improve information security | Yes |  |
| A.5.36 | Compliance with policies and standards for information security | Yes | Yes<br>18.2.2<br>18.2.3 | Safeguarding information security | Yes |  |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.5.37 | Documented operating procedures | Yes | Yes<br>12.1.1 | Guaranteeing continuity and security of services<br>Risk management: RA-2021-0064 and RA-2021-0056 | Yes | |

| A. 6 | People controls | Selected Yes / No | | If selected, reason for inclusion | Implemented Yes / No | If not selected, reason for exclusion |
|---|---|---|---|---|---|---|
| | | ISO 27001 :2022 | ISO 27017 :2015 | | | |
| A.6.1 | Screening | Yes | Yes<br>7.1.1 | Responsibility towards customers, suppliers and organization.<br>Risk management RA-2022-0010 | Yes | |
| A.6.2 | Terms and conditions of employment | Yes | Yes<br>7.1.2 | Responsibility towards customers, suppliers and organisation<br>Legislation: Balanced Labour Market Act (Wet Arbeidsmarkt in balans)<br>Risk management RA-2021-0024, RA-2021-0022, RA-2021-0021 and RA-2021-0015 | Yes | |
| A.6.3 | Information security awareness, education and training | Yes | Yes<br>7.2.2<br>CSC<br>CSP | Responsibility towards customers, suppliers and organisation | Yes | |
| A.6.4 | Disciplinary process | Yes | Yes<br>7.2.3 | Responsibility towards customers, suppliers and organisation | Yes | |
| A.6.5 | Responsibilities after termination or change of employment | Yes | Yes<br>7.3.1 | Controlled access to corporate resources based on individual privileges | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Legislation: GDPR, Data Breach Notification Act (Wet Meldplicht Datalekken), Wbni and NIS2. | | |
| A.6.6 | Confidentiality or non-disclosure agreements | Yes | Yes<br>13.2.4 | Protecting sensitive (business) information<br>Contractual requirements for customers<br>Risk management RA-2021-0014, RA-2021-0007 and RA-2021-0006 | Yes | |
| A.6.7 | Remote working | Yes | Yes<br>6.2.2 | In line with working from home policy | Yes | |
| A.6.8 | Information security event reporting | Yes | Yes<br>16.1.2<br>CSC<br>CSP<br>16.1.3 | Transparency towards customers, Terms and conditions with customers.<br>Legislation: Data Breach Notification Act (Wet Meldplicht Datalekken), GDPR, Wbni and NIS2. | Yes | |

| A. 7 | Physical controls | Selected Yes / No | | If selected, reason for inclusion | Implemented Yes / No | If not selected, reason for exclusion |
|---|---|---|---|---|---|---|
| | | ISO 27001 :2022 | ISO 27017 :2015 | | | |
| A.7.1 | Physical security perimeter | Yes | Yes<br>11.1.1 | Controlled access to corporate resources based on individual privileges | Yes | |
| A.7.2 | Physical entry controls | Yes | Yes<br>11.1.2<br>11.1.6 | Controlled access to corporate resources based on individual privileges | Yes | |
| A.7.3 | Securing offices, rooms and facilities | Yes | Yes | Controlled access to | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | 11.1.3 | corporate resources based on individual privileges | | |
| A.7.4 | Physical security monitoring | No | Not in norm | | No | Other measures cover the risks of damage due to burglary/theft |
| A.7.5 | Protecting against physical and environmental threats | Yes | Yes<br>11.1.4 | Ensuring continuity of service<br>Risk management: RA-2021-0068, RA-2021-0060, RA-2021-0050, RA-2021-0049 and RA-2021-0002 | Yes | |
| A.7.6 | Working in secure areas | Yes | Yes<br>11.1.5 | Ensuring the safety of critical business resources | Yes | |
| A.7.7 | Clear desk and clear screen | Yes | Yes<br>11.2.9 | Safeguarding the confidentiality of sensitive (business) information<br>Risk management: RA-2021-0028, RA-2021-0025 | Yes | |
| A.7.8 | Equipment siting and protection | Yes | Yes<br>11.2.1 | Ensuring the safety of critical business resources | Yes | |
| A.7.9 | Security of assets off-premises | Yes | Yes<br>11.2.6 | Ensuring the safety of critical business resources | Yes | |
| A.7.10 | Storage media | Yes | Yes<br>8.3.1<br>8.3.2<br>8.3.3<br>11.2.5 | Safeguarding the confidentiality of sensitive (business) information | Yes | |
| A.7.11 | Supporting utilities | Yes | Yes<br>11.2.2 | Ensuring continuity of service<br>Risk management: RA-2022-0011 | Yes | |
| A.7.12 | Cabling security | Yes | Yes<br>11.2.3 | Safeguarding the security of sensitive (business) information | Yes | |
| A.7.13 | Equipment maintenance | Yes | Yes<br>11.2.4 | Safeguarding the security of sensitive (business) | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | information | | |
| A.7.14 | Secure disposal or re-use of equipment | Yes | Yes<br>A.11.2.7 CSC<br>CSP | Safeguarding the security of sensitive (business) information. Preventing License Agreement Violations | Yes | |

| A. 8 | Technological controls | Selected Yes / No | | If selected, reason for inclusion | Implemented Yes / No | If not selected, reason for exclusion |
|---|---|---|---|---|---|---|
| | | ISO 27001 :2022 | ISO 27017 :2015 | | | |
| A.8.1 | User endpoint devices | Yes | Yes<br>6.2.1<br>11.2.8 | Safeguarding the security of sensitive (business) information. | Yes | |
| A.8.2 | Privileged access rights | Yes | Yes<br>9.2.3<br>CSC<br>CSP | Controlled access to corporate resources based on individual privileges | Yes | |
| A.8.3 | Information access restriction | Yes | Yes<br>9.4.1<br>CSC<br>CSP | Controlled access to corporate resources based on individual privileges<br>Risk management: RA-2021-0070 | Yes | |
| A.8.4 | Access to source code | Yes | Yes<br>9.4.5 | Controlled access to company resources based on individual privileges Risk management: RA-2021-0019 | Yes | |
| A.8.5 | Secure authentication | Yes | Yes<br>9.4.2 | Controlled access to corporate resources based on individual privileges | Yes | |
| A.8.6 | Capacity management | Yes | Yes<br>12.1.3 | Ensuring continuity of | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | CSC<br>CSP | service Risk management: RA-2021-0036 | | |
| A.8.7 | Protection against malware | Yes | Yes<br>12.2.1 | Safeguarding the security of sensitive (business) information.<br>Risk management: RA-2021-0067, RA-2021-0059, RA-2021-0048, RA-2021-001 | Yes | |
| A.8.8 | Management of technical vulnerabilities | Yes | Yes<br>12.6.1<br>CSC<br>CSP<br>18.2.3 | Guaranteeing continuity and security of services<br>Risk management: RA-2021-0053, RA-2024-0047, RA-2021-0041, RA-2021-0040 | Yes | |
| A.8.9 | Configuration management | Yes | Not in norm | Risk management: RA-2024-0012<br>Guaranteeing continuity and security of services | Yes | |
| A.8.10 | Information deletion | Yes | Not in norm | Risk management: RA-2024-0013<br>Safeguarding the security of sensitive (business) information. | Yes | |
| A.8.11 | Data masking | Yes | Not in norm | Risk management: RA-2024-0013<br>Safeguarding the security of sensitive (business) information.<br>Legislation: GDPR | Yes | |
| A.8.12 | Data leakage prevention | Yes | Not in norm | Risk management: RA-2021-0033<br>Safeguarding the security of sensitive (business) information. | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.8.13 | Information backup | Yes | Yes<br>12.3.1<br>CSC<br>CSP | Safeguarding the security of sensitive (business) information.<br>Risk management: RA-2023-0003, RA-2023-0002, RA-2021-0035, RA-2021-0029, RA-2021-0029, RA-2021-0018, RA-2021-0017 | Yes | |
| A.8.14 | Redundancy of information processing facilities | Yes | Yes<br>17.2.1 | Ensuring continuity of service<br>Risk management: RA-2024-0004, RA-2024-0003, RA-2024-0002, RA-2024-0001, RA-2022-0009, RA-2022-0008, RA-2022-0006, RA-2022-0005, RA-2022-0004, RA-2022-0003, RA-2021-0034, RA-2021-0012 | Yes | |
| A.8.15 | Logging | Yes | Yes<br>12.4.1<br>CSC<br>12.4.2<br>12.4.3<br>CSC | Ensuring continuity and safety of services Risk management: RA-2021-0061, RA-2021-0008 | Yes | |
| A.8.16 | Monitoring activities | Yes | Not in norm | Risk management: RA-2021-0059, RA-2021-0009<br>Guaranteeing continuity and security of services | Yes | |
| A.8.17 | Clock synchronisation | Yes | Yes<br>12.4.4<br>CSC<br>CSP | Safeguarding integrity of security measures | Yes | |
| A.8.18 | Use of privileged utility programs | Yes | Yes<br>9.4.4<br>CSC | Ensuring the effectiveness of safety measures<br>Risk management: RA- | Yes | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  |  | CSP | 2022-0012 |  |  |
| A.8.19 | Installation of software on operational systems | Yes | Yes<br>12.5.1<br>12.6.2 | Guaranteeing continuity and security of services | Yes |  |
| A.8.20 | Network controls | Yes | Yes<br>13.1.1 | Guaranteeing continuity and security of services | Yes |  |
| A.8.21 | Security of network services | Yes | Yes<br>13.1.2 | Guaranteeing continuity and security of services | Yes |  |
| A.8.22 | Segregation in networks | Yes | Yes<br>13.1.3<br>CSC<br>CSP | Reducing the impact of disruptions, ensuring the security of (company) data | Yes |  |
| A.8.23 | Web filtering | Yes | Not in norm | Risk management: RA-2024-0015<br>Limiting safety risks in workplaces | Yes |  |
| A.8.24 | Use of cryptography | Yes | Yes<br>10.1.1<br>CSC<br>CSP<br>10.1.2<br>CSC | Safeguarding the safety of (company) data Risk management: RA-2023-0004 | Yes |  |
| A.8.25 | Secure development lifecycle | Yes | Yes<br>14.2.1<br>CSC<br>CSP | Guaranteeing the security of your own software<br>Risk management: RA-2021-0005 | Yes |  |
| A.8.26 | Application security requirements | Yes | Yes<br>14.1.2<br>14.1.3 | Guaranteeing the security of your own software<br>Risk management: RA-2021-0004, RA-2021-0003 | Yes |  |
| A.8.27 | Secure system architecture and engineering principles | Yes | Yes<br>14.2.5 | Guaranteeing the security of your own software | Yes |  |
| A.8.28 | Secure coding | Yes | Not in norm | Risk management: RA-2024-0016 | Yes |  |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Guaranteeing the security of your own software | | |
| A.8.29 | Security testing in development and acceptance | Yes | Yes<br>14.2.8<br>14.2.9 | Guaranteeing the security of your own software | Yes | |
| A.8.30 | Outsourced development | Yes | Yes<br>14.2.7 | Diesis: Interests and risks for own development also apply to outsourced development | Yes | Other companies do not have outsourced development |
| A.8.31 | Separation of development, test and production environments | Yes | Yes<br>12.1.4<br>CSC<br>14.2.6 | Safeguarding the security of (company) data<br>Risk management: RA-2021-0016 | Yes | |
| A.8.32 | Change management | Yes | Yes<br>12.1.2<br>CSP<br>14.2.2<br>14.2.3<br>14.2.4 | Ensuring continuity and security of our own software Risk management: RA-2021-0011 | Yes | |
| A.8.33 | Test information | Yes | Yes<br>14.3.1 | Safeguarding the security of (company) data | Yes | |
| A.8.34 | Protection of information systems during audit and testing | Yes | Yes<br>12.7.1 | Safeguarding the security of (company) data | Yes | |

| | ISO 27017 specific measures | Selected Yes / No | If selected, reason for inclusion | Implemented Yes / No | If not selected, reason for exclusion |
|---|---|---|---|---|---|
| CLD | | ISO 27017:2015 | | | |
| 6.3.1 | Shared roles and responsibilities within a cloud computing environment | Yes | Ensure that the management of the cloud stack aligns. | Yes | Quintensis does not take part in 27017 certification. |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| 8.1.5 | Removal of cloud service customer assets | Yes | From a processing agreement and guaranteeing customer continuity. | Yes | Quintensis does not take part in 27017 certification. |
| 9.5.1 | Segregation in the virtual computing environment | Yes | Ensuring the confidentiality of customer data. | Yes | Quintensis does not take part in 27017 certification. |
| 9.5.2 | Virtual machine hardening | Yes | Reduce the risk of vulnerabilities. | Yes | Quintensis does not take part in 27017 certification. |
| 12.1.5 | Administrator's operational security | Yes | Guaranteeing continuity and security of services | Yes | Quintensis does not take part in 27017 certification |
| 12.4.5 | Monitoring of cloud services | Yes | Providing transparency to customers | Yes | Quintensis does not take part in 27017 certification |
| 13.1.4 | Alignment of security management for virtual and physical networks | Yes | Guaranteeing the safety of services | Yes | Quintensis does not take part in 27017 certification |

## 5. Signature

| Name | Company | Function | Signature |
|---|---|---|---|
| Erik van Doorn Sr. | 4CEE | Group CEO | |
| Anton Rademakers | 4CEE | CFO | |
| Vincent Wouters | ICreative B.V. | CEO | |
| Jan Willem ter Steege | Easy Systems B.V. | CEO | J.W. ter Steege |
| Tino Wendriks | Diesis Consultancy B.V. | CEO | |
| Erik van Doorn | Stiply B.V. | CEO | |
| Erik van Doorn sr. | Quintensis B.V. | CEO | |