



Corporate Governance Statement 2017 ICT Group N.V.

This is the Corporate Governance statement as referred to in article 2a juncto article 3 until 3b of the 'Besluit nadere voorschriften inhoud jaarverslag' (hereinafter 'Decree'). The information required to be included in this corporate governance statement as described in articles 3, 3a and 3b of the Decree can be found below and in several sections of the Annual Report of ICT Group N.V. 2017 (hereinafter ICT).

The Dutch corporate governance code can be found on www.commissiecorporategovernance.nl

Information concerning compliance with the Dutch Corporate Governance Code, as required by article 3 of the Decree

ICT complies with the provisions of the Dutch Corporate Governance Code, with only a few deviations as described below. The Dutch Corporate Governance Code is available at www.mccg.nl.

Best practice provision 2.7.2 (ii): There is no regulation covering private investments by members of the Supervisory Board or members of the Executive Board other than securities issued by ICT Group N.V. Members of these boards are already subject to general legislation and regulations.

Best practice 3.4.1: Performance criteria for the variable remuneration of members of the Executive Board are described in general terms but not fully disclosed, as they contain sensitive information and could contain information of an otherwise confidential nature that ICT may not want to disclose.

Best practice 4.2.3.: Meetings between ICT and analysts, the press and/or investors will not be webcast due to cost considerations. The dates of the analyst and press meetings will be published on the website in advance and the presentation will be made available on the website.

Information concerning ICT's risk management and control frameworks relating to the financial reporting process, as required by article 3a sub a of the Decree

Introduction

ICT's risk management is the responsibility of the Executive Board. Risk management forms an integral part of the company's strategy. The main objective is to control and mitigate the most significant risks that ICT is or may be exposed to, while at the same time facilitating the realisation of operational and financial objectives. ICT continuously evaluates its internal controls and takes measures to improve these controls where necessary. The Executive Board discusses the risk management framework regularly with the Audit Committee and the Supervisory Board. In 2017, ICT took significant steps to further strengthen the risk and internal control framework. The position of Chief Information Security Officer was implemented to reflect the increasing importance of information security within the ICT Group. Risks related to information cyber security have been

added to the risk framework and are reflected in the risk impact/probability chart and risk overview presented in this chapter. Furthermore, it was decided to implement an internal audit function within the Group due to the company's growth and the consequential increased need for process improvements and alignment.

Risk management and control systems

ICT has implemented internal risk management and risk control systems with a view to minimising its operating and financial risks and to limit the impact of unexpected events on balance sheet ratios and results. ICT considers risk management to be a continuous process, an essential part of which is to embed policy in control systems and procedures at every level of the organisation.

ICT's internal framework is based on Entity-level controls:

Category	Important Elements
1. Control Environment	<ul style="list-style-type: none"> - Management's philosophy, attitude and tone at the top - Organisational structure, key areas of authority and lines of reporting - Knowledge & skills, policies & procedures - Oversight by Executive Board and Supervisory Board, responsibility for internal controls
2. Entity-wide Risk Assessment Process	<ul style="list-style-type: none"> - Identifying business risks - Evaluation of external and Internal Information - Review of regular financial reports and ad-hoc reporting - Approval of budgets, business planning documents and the business strategy
3. Communication	<ul style="list-style-type: none"> - Internal communication: Identification and communication - External communication: Preparation and review
4. Monitoring of Controls	<ul style="list-style-type: none"> - Maintaining a monitoring process for entity-level and process-level controls - Change of controls - Evaluating KPIs and financial reporting results - Testing the effectiveness of controls

Important elements of ICT's Control Framework

Planning and control cycle

Risk management is an integral part of the planning and control cycle. This system includes the determination of the strategy and the budget and is the responsibility of the Executive Board. The Executive Board discusses the strategy extensively with the Supervisory Board every year. The Executive Board then translates strategic objectives into business plans and budgets in cooperation with the directors of ICT's subsidiaries. The business plan contains both a financial budget and a number of concrete business objectives per legal entity and underlying business units. These objectives are translated into Key Performance Indicators (KPIs), which are measured for progress throughout the year. Important KPIs at ICT include the capacity utilisation rate, tariffs, numbers of direct and indirect FTEs and the efficiency of the company's processes. Management evaluates these key performance indicators and financial and operational reporting to identify any deficiencies in internal controls and to monitor results.

Policies and guidelines

Management creates and maintains a culture of integrity and ethical behaviour by setting the right tone at the top. This is done by:

- Leading by example;
- Clear corporate governance practices;
- A code of conduct, which includes relevant policies such as prohibiting employees from accepting gifts from suppliers;
- A whistleblower policy;
- A quality system used to document all of ICT's significant processes.

ICT's management is receptive to employees' ethical concerns and is committed to responding appropriately to misconduct. Management demonstrates adherence through their work practices and decisions. Management enforces its views through a combination of policies and procedures. When changes are made, employees are notified, and changes are implemented. Management does not provide incentives or offer temptations that might prompt personnel to engage in dishonest, illegal or unethical acts. A whistleblowing policy is in place and personnel can report suspected incidents anonymously.

ICT implemented an internal procedure, the so-called letters of representation, requiring ICT management to confirm compliance with ICT's policies and procedures. Given the growth of the company through acquisitions this process is increasingly important. This helps to provide the assurance the Executive Board needs to make its own in control statement. Responsibility and accountability for implementing systems and controls, including fraud prevention and detection, has been designated to ICT's Finance department and is embedded in the Internal Control Framework.

Performance and quality controls

Quality management is another important pillar of the company's risk management. ICT constantly works on improving the services that it provides to customers in whatever form. Providing services in accordance with accepted standards is embedded in the organisation as a regular process. ICT has adopted various standards, including ISO standards for information security and quality management and standards related to process maturity and safety, health and the environment. Furthermore, ICT continuously monitors the measurement of and reporting on the effectiveness and efficiency of measures taken. ICT regularly evaluates this via an audit by external parties (according to the above-mentioned standards), as well as through an internal review process related to effectiveness, suitability and correspondence with agreed norms. No critical findings have come to light in the various reviews.

Monitoring

ICT provides for optimal monitoring and timely identification of risks and, if necessary, mitigation of any risks that arise, through a constant process of internal controls and measurements. This risk management system with its control mechanisms and mitigating measures is a periodically recurring item on the agenda of the Audit Committee and, by extension, the Supervisory Board.

Sensitivity analysis

The table below illustrates the impact of changes in ICT's revenues, operating expenses, net debt and the interest rates.

	Change	Impact	On	Assumption
Revenue	+/-1%	+/- € 1.0 million	EBITDA	Flat gross margin and no change to cost base
Operating expenses	+/-1%	+/- € 0.8 million	EBITDA	
Interest rate	+100 bps	+ € 0.1 million	Financial charges	Average net debt 2017
Net debt	+/- € 3 million	+/- € 0.1 million	Financial charges	Stable interest rates

Improvements in the risk management and control systems in 2017

In 2017, ICT took significant steps to further strengthen its risk management and controls:

Full integration recent acquisitions

In 2017, we completely integrated both Nozhup, one of ICT's largest acquisitions, and HTS within ICT Netherlands. Both entities have been integrated within ICT Automatisering Nederland B.V. The people and processes now operate fully in line with the ICT Group policies and guidelines. BMA and Raster – both acquired before 2017 - operate autonomously within the ICT Group but were aligned this year with ICT's back offices systems, including the HR and Financial systems.

Cyber security

Cyber security can pose significant risks to both ICT and its customers. ICT appointed a Chief Information Security Officer (CISO), who is responsible for developing strategy and policies aimed at information security, implementation and monitoring of information security and data privacy. The CISO will direct information security for the whole Group and fulfils a central role in managing all processes involved.

Internal controls

The control framework was expanded to include all ICT subsidiaries. In 2017, the focus was on the implementation of the internal controls in the field of cyber security and data protection.

Internal audit

In 2017, the Supervisory Board, based on the Audit Committee's advice, decided that a formal internal audit function be created with the appointment of an internal auditor in 2018, reporting to the CEO and the Audit Committee.

Integrated reporting

In 2017, ICT took the first steps towards integrated reporting. The Executive Board, in consultation with the Supervisory Board, defined ICT's long-term value creation model. Furthermore, the company conducted a stakeholder assessment. Based on the dialogue with stakeholder groups, the company defined the material topics for ICT. These material topics are in line with the company's risk framework, as can be seen in the risk overview.

Insurance

ICT has added specific cyber and data protection insurance policies to its corporate insurance coverage.

Further certification

In 2017, ICT initiated ISO 27001 implementation for Strypes Bulgaria.

Given ICT's buy and build strategy and the ongoing expansion of the ICT Group, adequate internal controls are a continuous area of attention. Both the strengthening of the internal control framework at the existing ICT subsidiaries, as well as the implementation of the internal controls at newly (and to be) acquired and integrated entities require constant attention and additional steps. Given the company's growth path, implementing uniform processes and controls is important to safeguard the quality of ICT's solutions and services, which in turn is vital for sustainable longer-term growth. ICT has therefore identified the following focus areas for further improvement in 2018:

- Cyber security will continue to be one of the main focus areas.
- Further define and implement the internal audit function within the group. The search for the internal auditor has already commenced. The internal auditor will set up and lead ICT Group's Internal Audit Function and develop and execute a group-wide risk-based Internal Audit Plan in consultation with Executive Board, Audit Committee and external auditor.
- After strengthening the internal controls in the fields of finance, HR and Cyber security at our subsidiaries, in 2018 these controls will be further expanded to the operations of our subsidiaries. This means more process descriptions, improvement and alignment. Our internal audit function will be instrumental in this.
- Further steps in integrated reporting will be taken.

Key risk factors

ICT Group assesses all relevant risks according to the likelihood that they will occur and the impact they could have if they materialise, and ICT then assigns a weighting to those risks on that basis. The key risks we have identified are outlined below. For each risk, we indicate how these risks are mitigated, and specify our risk appetite for each risk. The order in which the risks are presented does not reflect their importance, probability or materiality. The actual occurrence of any of the following risks could have a material adverse effect on the company's business, prospects, operations, financial condition or results. All of these risks are contingencies, which may or may not occur.

Key business risks in 2017:

Cyber security risks

Digital security is crucial and nowadays affects every aspect of daily life, in business and society. Information security is becoming more and more important and the complexity will only increase. ICT's solutions are mostly embedded in the heart of its customers' operations. Digital risks involve issues such as privacy, phishing, cybercrime, internet fraud and even IT terrorism. ICT runs the risk of being fined if it does not comply with the new privacy legislation that comes into effect in 2018. Furthermore, the reputation risk can be very significant.

Clear policies and procedures are necessary to mitigate these risks. Providing its services in accordance with accepted standards is embedded in the organisation as a regular process. ICT has

adopted various standards and obtained a number of certifications, including ISO standards for information security (ISO 27001), medical devices (ISO 13485) and quality management and standards (ISO 9001) related to process maturity and safety, health and the environment. Furthermore, information security requires central coordination. Not only within ICT Automatisering Nederland B.V., but also in coordination with our other subsidiaries. The newly appointed Chief Information Security Officer plays a pivotal role in this.

Creating awareness, not only among our own people, but also at the customer, is also vital in mitigating these risks. Every new employee receives training on information security management.

Acquisitions

ICT's growth strategy is based on both organic growth and growth through acquisitions. This strategy does entail the risk of poor integration of acquisitions. In the event that ICT acquires companies, its ultimate objective is to adequately integrate these companies into the ICT Group. When acquiring a company, there is a risk of an undesired outflow of staff and drop off of operational performance. In addition, market circumstances and forecasts may sometimes necessitate the impairment of goodwill on acquisitions. However, ICT is building a track record in the successful integration of newly-acquired companies. This was demonstrated particularly well in 2017, with the smooth integration of one of ICT's largest acquisitions, Nozhup.

Labour market scarcity

The ability to attract and retain the right people is a key driver of growth. And this is becoming more crucial as talent is increasingly scarce. ICT strives to be an attractive employer that invests in its people and encourages entrepreneurship. ICT continuously develops and implements initiatives to reinforce this. "Bring out the best in yourself" is how ICT approaches its HR development strategy. Important elements in this approach are employee empowerment and entrepreneurship. ICT's approach to being the employer of choice is further elaborated on in the section ICT – an ambitious employer.

Labour market scarcity also results in incremental costs to attract highly talented people. These costs can result in the risk of serious margin pressure. ICT tries to mitigate this risk by continuously moving up the value chain, where additional margin can be realised. We are also shifting toward more scalable projects and selling an increasing number of solutions. ICT has always been known for its high quality and this should also translate into higher fees. And lastly, ICT tries to create awareness at its customers that as talent is becoming increasingly scarce, it is also becoming more expensive.

New business development

Innovation is very important for the future development of the company. The pace of the new technological developments is constantly increasing. ICT's focus on new business development, in combination with an acceptable risk level, is reflected in the company's commitment to invest 1.5% of turnover in R&D. However, new business development initiatives carry a higher risk. In particular, the impact can be even higher in initiatives where ICT has different roles, such as technology partner, supplier or customer of start-ups. This relationship with start-ups can lead to financial risk (bad debt or impairment risk).

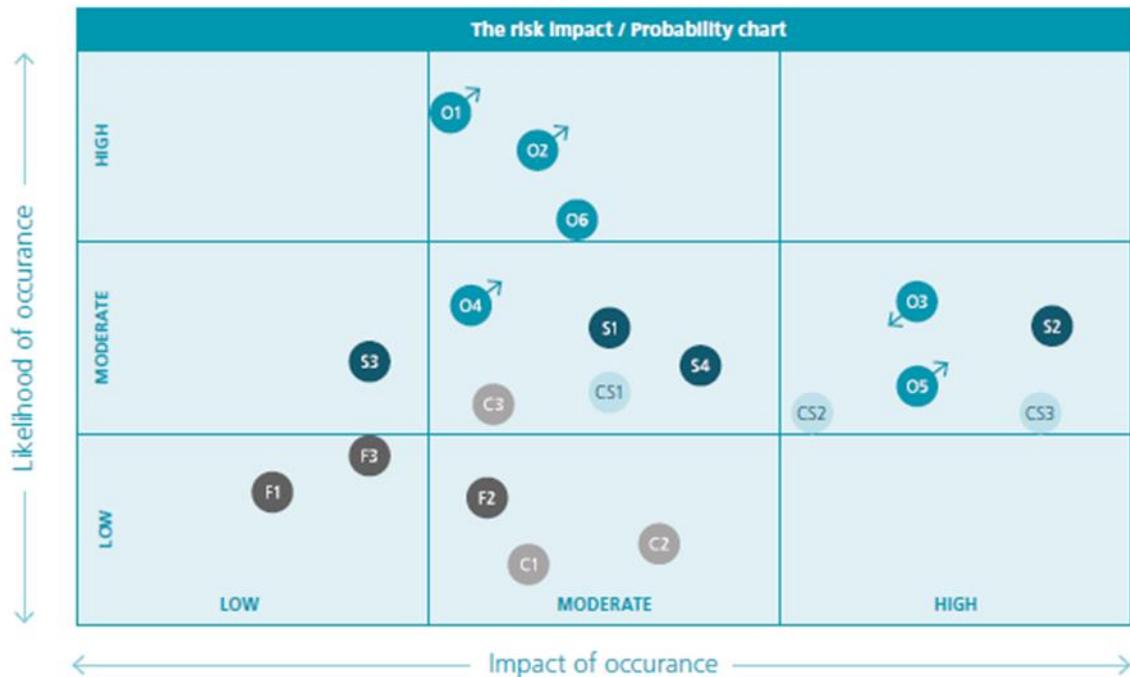
Inadequate project control

Projects can be complex due to the scale, the desired functionality, the applied technology or the involvement of several parties. This can result in financial risks in projects for which ICT Group bears result responsibility. ICT works continuously on an optimally functioning internal quality and control system to minimise the risks related to the execution of projects and assignments. To ensure continuity in the event of claims, ICT has a general and professional liability insurance. As the projects ICT is involved with are increasing in size, both the impact and the probability of the associated risks are likely to increase and will be addressed with appropriate risk mitigation measures.

These developments and trends can also be seen in the map below:

Impact and trends risks in 2017

The risk impact / Probability chart



- **Strategic risks**
 - S1: Sensitivity to economic cycles
 - S2: Speed of technological developments
 - S3: Multidimensional relationships
 - S4: New business development / start ups

- **Operational risks**
 - O1: Shortage of qualified staff
 - O2: Incremental costs to attract highly talented people
 - O3: Dependence on large clients
 - O4: Inadequate project control
 - O5: Unsuccessful integration of acquisitions
 - O6: New business models

- **Cyber Security risk**
 - CS1: Unauthorised access to ICT systems
 - CS2: Unauthorised access to customer systems
 - CS3: data breach

- **Financial risks**
 - F1: Reporting risks
 - F2: Inadequate funding
 - F3: Credit risk

- **Compliance risks**
 - C1: Failure to comply with legislation
 - C2: Fraud and corruption
 - C3: Increased potential liabilities

↗ ↖ Shows movement in comparison with 2016

Principal risk areas

The following overview of the principal risks for ICT is not exhaustive. It is also possible that risks that have not currently been identified, or that are not regarded as material, will have a significantly adverse effect on ICT's ability to achieve its objectives at a later date. ICT's internal risk management and risk control systems are, in as far as possible, geared to the timely identification of such risks.

Key risks		Mitigation	Risk appetite
Strategic risks			
S1	<i>Sensitivity to economic cycles</i>	<ul style="list-style-type: none"> - Maintain a leading position - Develop appropriate solutions as effectively and efficiently as possible - Make clear choices regarding strategic positioning - Spread activities across different markets, mix between different themes - Continuous monitoring of sales funnel and horizon 	<i>Low to Moderate</i>
S2	<i>Speed of technological developments</i>	<ul style="list-style-type: none"> - Alert response to changes affecting clients and markets - Invest in new technologies, products and people - Continuous training and education of professional staff - Partnerships to stay at the forefront of technological developments 	<i>Moderate</i>
S3	<i>Multi-dimensional relationships</i>	<ul style="list-style-type: none"> - Limit the exposure to 1.5% of annual revenue - Periodic monitoring of the mix and exposure to multi-dimensional relationships - Regular reviews with management of associated companies 	<i>Low to Moderate</i>
S4	<i>New business development, including collaboration with start-ups</i>	<ul style="list-style-type: none"> - Disciplined approach with start-ups - Limit the outstanding receivables related to start-ups 	<i>Low to Moderate</i>
Operational risks			
O1	<i>Shortage of well-qualified staff and inability to retain qualified staff</i>	<ul style="list-style-type: none"> - HR policy aimed at making ICT the employer of choice - Enable entrepreneurship and initiatives - Create a sufficiently challenging environment - Invest in relationships with schools and universities 	<i>Low</i>
O2	<i>Incremental costs to attract highly talented people</i>	<ul style="list-style-type: none"> - Offering higher added value solutions - Maintain high quality - More scalable projects - Increase awareness at customers that talent is becoming more expensive 	<i>Moderate</i>
O3	<i>Dependence on large clients</i>	<ul style="list-style-type: none"> - Broaden the client base, invest in sales - Offer more added value to increase clients' dependency on ICT 	<i>Moderate</i>
O4	<i>Inadequate project and assignment control</i>	<ul style="list-style-type: none"> - Continuous improvement of internal quality and control systems - Qualified management with adequate competencies and business and IT knowledge - Continuous training and education of project staff 	<i>Low to Moderate</i>
O5	<i>Unsuccessful integration of acquisitions or joint ventures</i>	<ul style="list-style-type: none"> - Prudent decision-making process in acquisition phase - Disciplined and standardised integration process, including connectivity to ICT's enterprise systems - A welcome programme for new colleagues 	<i>Moderate</i>

O6	<i>New business models / license selling, software as a service</i>	<ul style="list-style-type: none"> - Close involvement of legal department and external legal advice where needed - Apply lean start-up methodology with frequent reviews and interventions 	<i>Low to Moderate</i>
Cyber security risks			
CS1	<i>Unauthorised access to ICT systems</i>	<ul style="list-style-type: none"> - Continuously increase resilience of the ICT systems - Ongoing security testing - Ongoing awareness training and programs for ICT staff 	<i>Low</i>
CS2	<i>Unauthorised access to (ICT developed) customer systems</i>	<ul style="list-style-type: none"> - Security & privacy protocols as integral part of delivery of systems - Increase awareness at customer through training - ISO 27001 certifications 	<i>Low</i>
CS3	<i>Data breach</i>	<ul style="list-style-type: none"> - Update and implementation of data breach and privacy policies - Clear procedures are in place for data collection and storage - Ongoing awareness training and programmes on own platforms - Regular audits 	<i>Low</i>
Financial risks			
F1	<i>Reporting risks</i>	<ul style="list-style-type: none"> - Internal procedures and guidelines for internal and external reporting (Internal Control Framework) - External audit and supervision by the Audit Committee - Implementation of a consolidation tool - Internal letter of representation process in place 	<i>Low</i>
F2	<i>Inadequate funding</i>	<ul style="list-style-type: none"> - Ensure adequate financing facilities, both for acquisitions and working capital - Operate well within the covenants agreed with the banks 	<i>Low</i>
F3	<i>Credit risk</i>	<ul style="list-style-type: none"> - New customers are analysed individually for creditworthiness, including external ratings - Global credit insurance for all group companies 	<i>Low</i>
Compliance risks			
C1	<i>Failure to comply with laws and legislation</i>	<ul style="list-style-type: none"> - Continuous monitoring of laws and regulations - Close involvement of legal department and external legal advice 	<i>Low</i>
C2	<i>Fraud and corruption</i>	<ul style="list-style-type: none"> - Internal Control Framework that includes various preventive and detective controls, including fraud aspects - Corporate governance system - Appropriate levels of delegation of authority to sign policy - Segregation of duties in main business processes 	<i>Low</i>
C3	<i>Increased potential liability following changes in contractual conditions (as a consequence of change in product / service mix)</i>	<ul style="list-style-type: none"> - Close involvement of legal department and external legal advice in contractual agreements - Appropriate general and professional liability insurance 	<i>Low</i>

Executive Board's in control statement

The Executive Board is responsible for the design and operation of the internal risk management and control systems. In discharging this responsibility, the Executive Board has made an assessment of the effectiveness of the design and operation of the internal control and risk management systems.

In accordance with best practice 1.4.3 of the Dutch corporate governance code of December 2016 and taking into account the aforementioned assessment, the Executive Board confirms to the best of its knowledge and belief, that:

- the report provides sufficient insights into any deficiencies in the effectiveness of the internal risk and control systems;
- the internal risk management and control systems of the company provide reasonable assurance that financial reporting does not contain any material inaccuracies;
- there is a reasonable expectation that ICT Group will be able to continue its operations and meet its liabilities for at least twelve months, therefore, it is appropriate to adopt the going concern basis in preparing the financial reporting;
- there are no material risks or uncertainties that could reasonably be expected to have a material adverse effect on the continuity of ICT Group's operations in the coming twelve months.

It should be noted that the above does not imply that these systems and procedures provide absolute assurance as to the realization of operational and strategic business objectives, or that they can prevent all misstatements, inaccuracies, errors, fraud and non-compliances with legislation, rules and regulations. Nor can they provide certainty that we will achieve our objectives.

Information regarding the functioning of ICT's general meeting of shareholders, and the authority and rights of ICT's shareholders, as required by article 3a sub b of the Decree

ICT Group N.V., a public limited liability company incorporated under Dutch law with its registered office in Barendrecht, the Netherlands (the "company") is the parent company of the ICT group of companies. The company's shares have been listed on Euronext Amsterdam since 1997. The company qualifies as a 'large company' (structuurvennootschap) within the meaning of the Dutch Civil Code and applies the relevant rules of Dutch corporate law.

General meeting of shareholders

An Annual General Meeting of Shareholders is held once a year in Barendrecht, Rotterdam or Amsterdam, such within six months of the end of the financial year. Extraordinary General Meetings of Shareholders may be convened by the Executive Board or the Supervisory Board if deemed necessary and by shareholders representing 10% of the issued capital after judicial authorisation. Meetings are convened by public notice sent by way of an announcement published electronically, which will be immediately and permanently accessible to the general meeting, for at least 42 days prior to the (Extraordinary) General Meeting of Shareholders. Those shareholders who alone or jointly represent at least 3% of ICT's issued share capital may request items be added to the agenda of the General Meeting of Shareholders. Such a request will be granted if it is received in writing at

least 60 days before the meeting, stating the reasons for said request. Every shareholder is entitled to attend the meeting and to speak and vote during the meeting. Each share carries one vote. An amendment of the Articles of Association requires the approval of the General Meeting of Shareholders.

Purchase and issue of (rights to) shares

The Annual General Meeting of Shareholders on 10 May 2017 resolved to authorise the Executive Board, subject to approval of the Supervisory Board, to acquire fully paid-up ordinary shares in the company's own capital to a maximum of 10% of the subscribed capital of the company within the limits of the Articles of Association for another 18 months as of 10 May 2017. In addition, the Annual General Meeting of Shareholders resolved to authorise the Executive Board, subject to the approval of the Supervisory Board, to issue shares or grant rights to acquire shares in the company, as well as to restrict or exclude the pre-emptive right pertaining to such shares for 18 months as of 10 May 2017. This authorisation is limited to a maximum of 10% of the number of shares issued as of 10 May 2017, plus 10% of the issued capital in connection with or on the occasion of mergers, acquisitions or strategic alliances.

In addition to the powers mentioned in this document, other specific powers and responsibilities of the General Meeting of Shareholders are described in the Articles of Association that are available on our website.

Information regarding the composition and functioning of ICT's Executive Board and the Supervisory Board, as required by article 3a sub c of the Decree:

Executive Board

The company has a two-tier board structure, comprising an Executive Board and a Supervisory Board. The Executive Board is responsible for the management of the company and for determining the long-term objectives and strategy, financing, compliance with relevant laws and regulations and the management of risks. In accordance with the company's objectives and Dutch law, the Executive Board manages the company, taking into account the interests of all relevant stakeholders. The Executive Board is supervised by the Supervisory Board. The Executive Board provides the Supervisory Board with all the information the Supervisory Board needs to fulfil its responsibilities. Certain decisions of the Executive Board require the approval of the Supervisory Board, as laid down in the Executive Board regulations, which can be found on the company's website. In addition to legal regulations, these regulations describe how the Executive Board works.

Appointment of members of the Executive Board

Members of the Executive Board are appointed by the Supervisory Board. The Supervisory Board shall inform the General Meeting of Shareholders and the Works Council in advance of a proposed appointment. The members of the Executive Board are appointed for a term of four years. This term expires at the end of the General Meeting of Shareholders to be held in the fourth year after the year of their appointment. Reappointment is possible for consecutive terms of four years.

Members of the Executive Board may be suspended or dismissed by the Supervisory Board. In the event of a dismissal, the General Meeting of Shareholders shall be consulted.

On 1 March 2017 the Executive Board consisted of mr J. Blejje (CFO and member of the Executive Board) and Mr. J.W. Wienbelt (CFO and member of the Executive Board).

Supervisory Board

The Supervisory Board is responsible for supervising and advising the Executive Board and overseeing the policies of the Executive Board and the general course of affairs of the company and its business. The Supervisory Board supervises how the Executive Board determines the long-term value creation strategy and how the Executive Board implements that strategy. Supervision also focuses on the set-up and operation of internal risk management and related control systems, the financial reporting processes, compliance with legislation and regulations, corporate social responsibility and the activities of the Executive Board regarding the culture within ICT. In fulfilling its responsibilities, the Supervisory Board is guided by the interests of the Company, its business and the interests of all relevant stakeholders.

Under Dutch law and in accordance with the provisions of the Code, the Supervisory Board is a separate body that is independent of the Executive Board and all its members are independent.

The Supervisory Board has two separate committees: the Remuneration and Appointment Committee and the Audit Committee. The Supervisory Board as a whole is responsible for the supervisory tasks. The Supervisory Board works according to the Supervisory Board regulations that include a detailed description of its tasks and responsibilities. These regulations also contain the tasks and responsibilities of the Remuneration and Appointment Committee and the Audit Committee and can be found on the company's website.

Appointment of members of the Supervisory Board

The members of the Supervisory Board are appointed by the General Meeting of Shareholders based on a nomination of the Supervisory Board. The Supervisory Board informs the general meeting and the works council simultaneously of the nomination. The general meeting and the works council may recommend to the Supervisory Board persons for nomination as supervisory directors. The Supervisory Board shall for that purpose inform the general meeting and the works council in a timely fashion when a vacancy is to be filled. The general meeting may reject the nomination of the Supervisory Board with an absolute majority of the votes cast, representing at least one-third of the issued capital.

For a third of the members of the Supervisory Board, the Works Council has the right to recommend a candidate. The Supervisory Board may object to this recommendation if it considers the recommended person to be unsuitable to fulfil the duties of a Supervisory Board member, or if it believes that the Supervisory Board would not be properly composed if the appointment were made according to said recommendation. The Supervisory Board must inform the Works Council of its objection and consult with the Works Council to reach agreement on the nomination. If no agreement can be reached, the Enterprise Chamber of the Amsterdam Court of Appeal can be asked to render a decision on the objection.

Members are appointed for a period of four years and may be re-elected for another four years in compliance with the Corporate Governance Code. A Supervisory Board member may thereafter be reappointed again for a period of two years and that appointment can in principle be extended by at most two years. In the event of a reappointment after an eight-year period, the reason for said reappointment will be explained in the report of the Supervisory Board. The members of the Supervisory Board can only be dismissed by the Enterprise Chamber of the Amsterdam Court of

Appeal. The entire Supervisory Board shall resign in the event the General Meeting of Shareholders adopts a motion of no confidence against the Supervisory Board. A Supervisory Board member may be suspended by the Supervisory Board; the suspension shall end by operation of law if the company has not applied to the Enterprise Chamber to remove the member within one month after the commencement of the suspension.

As per 1 March 2018, the Supervisory Board consists of Mr. Th. J. van der Raadt (chairman), Mr. F.J. Mr. J.A. Sinoo (vice chairman), Mr. Fröschl and Mr. D. Luthra. The Audit committee consists of Mr. D. Luthra (chairman) and Mr. J.A. Sinoo. Mr. J.A. Sinoo (chairman) and Mr. Th.J. van der Raadt together form the Remuneration and Appointments Committee.

Information on the diversity policy regarding the composition of the Executive Board and the Supervisory Board of ICT, as required by article 3a sub d of the Decree.

ICT aims for diversity not only in terms of experience, but also in terms of nationality, gender and age at all levels within the company.

The various members bring a wide range of skills and experience to the Supervisory Board from a broad range of backgrounds and industries. Two of the four members have non-Dutch nationality. With the exception of gender diversity, the composition of both the Executive and Supervisory Board is diverse.

The company currently does not have the desired allocation of seats to men and women on the Executive and Supervisory boards. There are currently no female members on the Executive Board, nor on the Supervisory Board. Any recommendation for appointments to the General Meeting of Shareholders takes into account experience, background and other diversity factors. ICT strives to have at least 30% females among the members of its Supervisory and Executive Boards. Subject to the appointment of Mrs. van der Werf by the General Meeting of Shareholders, female members will account for 25% of the Supervisory Board as of May 2018.

The aim for a diverse composition, and the specific gender target, also applies to the composition of the Executive Board and senior management. The Executive Board currently consists of Mr. J.H. Blejje and Mr. W.J. Wienbelt. With an Executive Board consisting of only two positions and an industry where female talent is scarce, it will not be easy to meet this 30% target. In view of the performance in the past four years, there is no intent to amend the composition of the Executive Board, nor to increase the number of Executive Board members. As such, ICT does not expect to meet the 30% target at the level of the Executive Board in the foreseeable future.

The Supervisory Board closely monitors the Executive Board's efforts to fostering female talent across the group, encouraging women's networks and mentoring programmes, together with the promotion of gender equality in general.

The information concerning the inclusion of the information required by the decree Article 10 EU Takeover Directive, as required by article 3b of the Decree:

This information is included in this document and the Annual Report 2017 in the sections shareholder information, corporate governance and remuneration report.

Barendrecht 1 March 2018