Principal risks and uncertainties
Mitigation that helps us to deliver our strategy

1. Risk overview/landscape
Our long-term success is built on a clear strategic direction, contractual and operational excellence, and effective back office functions, such as Finance and Human Resources, enabling customer-facing staff to fulfil their obligations effectively. All of this is underpinned by a secure IT infrastructure, hosting both internal and customer platforms. Our strategic, contractual and infrastructure risks are largely determined by the industry we operate in and our long-term approach to adding value. Our financial and people risks are defined by the wider economic environment, the way we run our business day-to-day and our long-term staffing needs. While outside factors are beyond our control, our risk management approach is committed to managing the impact of these influences, while controlling the internal elements vital to our success.

2. Risk appetite
Our risk appetite is strongly influenced by our experience in the industry sector in which we operate. At an operational level, we have a higher risk appetite for business development where we have experience of the risks and a lower risk appetite where we have less experience. This is supported day-to-day by our operating policies and governance processes.

3. Risk culture
Risk management and governance processes are well-established and understood within the business and operate at all levels. Strategic-level risks are monitored by the Risk and Audit Committees, as well as by the Board. Lower level operational risks are identified, analysed and mitigated at a functional level on an ongoing basis, using well-embedded processes.

4. Risk identification and impact
The Group Risk Committee reviews our principal risks on an annual basis. These risks are the barriers to meeting our strategic goals. This top-down approach includes assessing whether emerging risks are significant enough to warrant inclusion on the Group Risk Log. If so, the likelihood of occurrence and potential impact are considered and the risk is subject to regular review. The impact of existing risks is also reviewed. The key risks are further considered in relation to the Long-Term Viability Statement.

5. Risk trends
The overall risk landscape has remained relatively static over the year.

Strategic: The strategic-level risk profile is one of long-term risk due to technological change and Computacenter’s ability or otherwise to innovate effectively. It has decreased over the period, as our response has matured.

Contractual/Operational: We recognised a new risk in this category this year, in relation to compliance with the General Data Protection Regulation (GDPR), which will come into force in May 2018. We regularly review our progress with our compliance project.

Lower-level risks are identified and analysed through the Group Operating Business Risk Assessment process, the results of which are also reviewed by the Group Risk Committee.

Infrastructure: Although there has been no overall change in relation to impact or likelihood of occurrence, cyber security remains at the forefront of discussions at both the Risk and Audit Committees.

Financial: Risks relating to the departure of the UK from the EU remain under review. As the date of departure nears, we have established an executive-level committee to assess the potential risks in more detail and our response to them.

People: There has been no change to the risk profile, with both recruitment and succession planning remaining paramount to Computacenter’s future success.
**How Risk Links to Strategy**

Risk management is a process that helps maximise the chances of achieving our strategic objectives.

### Our Four Strategic Objectives

- **Strategic Objective 1:** To lead with and grow our Services business
- **Strategic Objective 2:** To improve our Services productivity and enhance our competitiveness
- **Strategic Objective 3:** To retain and maximise the relationship with our customers over the long term
- **Strategic Objective 4:** To innovate our Services offerings to build future growth opportunities

### Risk Categories:

- **Strategic Risk**
  - Adverse technology change
  - Inappropriate investment

- **Contractual Risk/Operational Risk**
  - Underdelivery on contractual commitments
  - Ineffective international business strategies
  - Untested design and pricing structures
  - GDPR compliance

- **Infrastructure Risk**
  - Cyber threat
  - Systems outages

- **Financial Risk**
  - Poor control of working capital
  - Poor control of direct costs
  - Underinvestment in indirect costs
  - UK’s departure from EU

- **People Risk**
  - Poor staff recruitment and retention
  - Inadequate succession planning

---

[Related material:
How it all fits together – page 17
Accountability – page 66]
1. STRATEGIC RISK

Alert status
Reduced likelihood

Risks
- Technology change dramatically reducing customer demand for our service and product offerings (CEO)
- Not investing appropriately or over-investing in the wrong automation, self-service and remote tools, when compared to our competition (CEO/GCOO)

Principal impacts
- Reduced margin
- Excess operational staff
- Contracts not renewed
- Missed business opportunities

Response to risk
- Well-defined Group strategy, backed up by an annual strategy process that considers our offerings against market changes
- Group Investment & Strategy Board considers strategic initiatives
- Additional measures including CEO-led country, sector and win/loss reviews

Risk owner
- Chief Executive Officer (CEO)
- Group Chief Operating Officer (GCOO)
### 2. CONTRACTUAL/OPERATIONAL RISK

**Alert status**
New risk in relation to GDPR

<table>
<thead>
<tr>
<th>Risks</th>
<th>Principal impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Failure to deliver against contractual commitments for our Services business (GCOO/GQAD/GHSM)</td>
<td>• Key decision makers failing to implement appropriate designs and pricing structures (CMD)</td>
</tr>
<tr>
<td>• Failure to deliver and manage our international business strategies effectively (HoI)</td>
<td>• Failure to comply with the General Data Protection Regulations (HL&amp;C)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response to risk</th>
<th>Principal impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mandatory governance processes relating to bids and new business take-ons substantively upgraded for Q1 2018. This includes risk-based decision-making assessments and new tooling</td>
<td>• Reduced margins</td>
</tr>
<tr>
<td>• Design and Delivery functions merged under the single leadership of the new Group Chief Operating Officer to establish better linkage between the two activities</td>
<td>• Loss-making contracts</td>
</tr>
<tr>
<td>• Board oversight of significant bids</td>
<td>• Reduced service and technical innovation</td>
</tr>
<tr>
<td>• New Group Head of Service Management appointed, to drive consistency and leverage Service Management best practice across the business</td>
<td></td>
</tr>
<tr>
<td>• Appointment of a Group Quality Assurance Director to provide independent quality assurance of key bids, key delivery programmes and to improve the extraction of value from our lessons learnt processes</td>
<td></td>
</tr>
<tr>
<td>• Regular commercial ‘deep dives’ into troubled contracts and challenging transformation projects</td>
<td></td>
</tr>
<tr>
<td>• Specialist International Management team</td>
<td></td>
</tr>
<tr>
<td>• Robust processes governing international business partners (subcontractors), before take-on and in-life, including alternate partners where applicable</td>
<td></td>
</tr>
<tr>
<td>• Project underway aimed at ensuring GDPR compliance</td>
<td></td>
</tr>
</tbody>
</table>

**Risk owner**

- Group Chief Operating Officer (GCOO)
- Country Managing Directors (CMD)
- Head of Legal & Contracting (HL&C)
- Group Head of Service Management (GHSM)
- Group Quality Assurance Director (GQAD)
- Head of International (HoI)
### 3. INFRASTRUCTURE RISK

**Alert status**
Unchanged risks, but some increase in activity levels

<table>
<thead>
<tr>
<th>Risks</th>
<th>Principal impacts</th>
<th>Response to risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber threat to Computacenter’s networks and systems, arising from</td>
<td>Inability to deliver business services</td>
<td>Well-communicated Group-wide information security and</td>
</tr>
<tr>
<td>either internal or external security breaches, leading to system</td>
<td>Reputational damage</td>
<td>virus protection policies</td>
</tr>
<tr>
<td>failure, denial of access or data loss. Cyber threats introduced by</td>
<td>Customer dissatisfaction</td>
<td>Specific inductions and training for staff working on</td>
</tr>
<tr>
<td>Computacenter to its customers’ networks and systems for whatever</td>
<td></td>
<td>customer sites and systems</td>
</tr>
<tr>
<td>reason (GCIO)</td>
<td></td>
<td>Specific policies and procedures for staff working</td>
</tr>
<tr>
<td></td>
<td></td>
<td>behind a customer’s firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ongoing and regular programme of external penetration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policies ensuring Computacenter does not run customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>applications or have access to customer data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regular review of cyber security controls</td>
</tr>
<tr>
<td>Failure leading to unacceptably long or regular short outages of</td>
<td></td>
<td>All Group standard systems built and operated on high</td>
</tr>
<tr>
<td>either internal or customer-facing systems (GCIO/GCOO)</td>
<td></td>
<td>availability infrastructure, designed to accommodate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>failure of any single technical component</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All centrally-hosted systems built and operated on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>high availability infrastructure, with multiple levels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of redundancy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All centrally-hosted systems benefit from dual network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connectivity into core datacenters designed to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>accommodate loss of network service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standing agenda item for consideration at each</td>
</tr>
<tr>
<td></td>
<td></td>
<td>meeting of the Group Risk Committee</td>
</tr>
</tbody>
</table>

**Risk owner**
• Group Chief Information Officer (GCIO)
• Group Chief Operating Officer (GCOO)
4. FINANCIAL RISK

Alert status
Unchanged risks

Risks
• Potential effect of UK’s departure from EU on our business as a result of anti-UK business sentiment, specific exit strategies or short-term issues such as foreign exchange volatility (GFD/GCOO)
• Underinvesting in our indirect costs, particularly Sales, leading to missed opportunities and top line impact (CMD)
• Poor control of debt management (GFD)
• Not taking advantage of productivity and cost reduction opportunities (GCOO)

Principal impacts
• Missed business opportunities
• Non-renewal of contracts
• Reduced revenue
• Reduced margin
• Financial impact through obsolete stock and/or bad debts
• Cost base too high compared to revenue

Response to risk
• Potential effect of UK’s departure from EU is subject to ongoing review by the Group Risk Committee, with particular short-term emphasis on foreign exchange volatility and hedging operations. New executive-level committee established to review risks and mitigations in more detail
• Commitment to excellent customer service and customer relations
• Deep understanding of the cost of service, allowing adjustable levels of service and customer price
• Implementation of debt management best practice following the centralisation of Group-wide collection functions at the Budapest Finance Shared Service Centre
• Monitor productivity, including KPIs on staff availability, utilisation, cross-charge efficiency and contractor ratio
• Enhanced tooling and subsequent reduction in manual activity to deliver cost reductions
• Monthly review by Management to assess sales teams’ ongoing performance and future effectiveness

Risk owner
• Group Finance Director (GFD)
• Group Chief Commercial Officer (GCCO)

5. PEOPLE RISK

Alert status
Unchanged risks

Risks
• Not recruiting and retaining the right calibre of staff across our customer-facing functions (GHRD)
• Inadequate succession planning or insufficient depth within key senior executive positions (GHRD/CEO)

Principal impacts
• Lack of adequate leadership
• Customer dissatisfaction
• Financial penalties
• Contract cancellations
• Reputational damage

Response to risk
• Succession planning in place for top 50 managers across the Group
• Regular remuneration benchmarking
• Incentive plans to aid retention
• Investment in management development programmes
• Regular staff surveys to understand and respond to employee issues

Risk owner
• Group Human Resources Director (GHRD)
• Chief Executive Officer (CEO)