SAFEGUARDING OUR FUTURE

Computacenter applies a rigorous and multi-layered approach to risk management. By blending appetite, model and process, we can manage and control our risks while remaining a customer-centric organisation.

We are well known for putting our customers first and empower our lead customer-facing people, to provide the flexibility and speed of response our customers want. Our governance process underscores this empowerment, by ensuring risks are identified and assessed at an appropriate level in the organisation.

It also allows for alignment with our overall risk appetite. We are often at the cutting edge of technology and services provision, and must balance our many business development opportunities with our ability to deliver and maintain our reputation for customer satisfaction and longevity of customer relationships. As a result, we have a healthy risk appetite for business development where we have experience of the risks and a lower risk appetite where we have less experience. Computacenter continuously applies this risk appetite, through both our risk management process and our Risk Governance Model.

The model and process comply fully with the UK Corporate Governance Code and the Financial Reporting Council Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.

Our model uses the well-defined Three Lines of Defence methodology:

- The First Line of Defence consists of operational management, who own the risks and apply the internal controls necessary for managing risks day-to-day.
- The Second Line of Defence offers guidance, direction and provides appropriate oversight and challenge. Internal compliance and assurance functions fall into this category.
- The Third Line of Defence, provided by Group Internal Audit, gives an independent view of the effectiveness of the risk management and internal control processes. It reports to the Audit Committee to ensure independence from management.

The main elements of our risk management process are as follows:

- The adherence to the Schedule of Matters Reserved for the Board ensures that all significant factors affecting Group strategy, structure, financing and contracts are addressed properly by the Directors.
- The Board and Executive Committee consider the principal risks which are the barriers to achieving the Board's strategic objectives.
- The Group Risk Committee, consisting of the Executive Directors, members of the Group Executive Committee and senior managers from across the Group, challenges the effectiveness of mitigations of the principal risks.
- The Group Risk Committee's deliberations, along with the current status of each principal risk, are reported to the Audit Committee and the Board.
- The Group Risk Committee considers each principal risk in-depth at least once a year, by receiving reports from the risk owner and challenging the mitigation approach.
- The principal risk list is reviewed once a year and leverages an annual operational risk review, where operational management identify their everyday risks.
- The Group Compliance Steering Committee, which was added to the governance model during 2016, assesses observance with laws and regulations, and reports to the Group Risk Committee.
- The bid governance process reviews bids or major changes to existing contracts, which aligns with our risk appetite and risk management process.

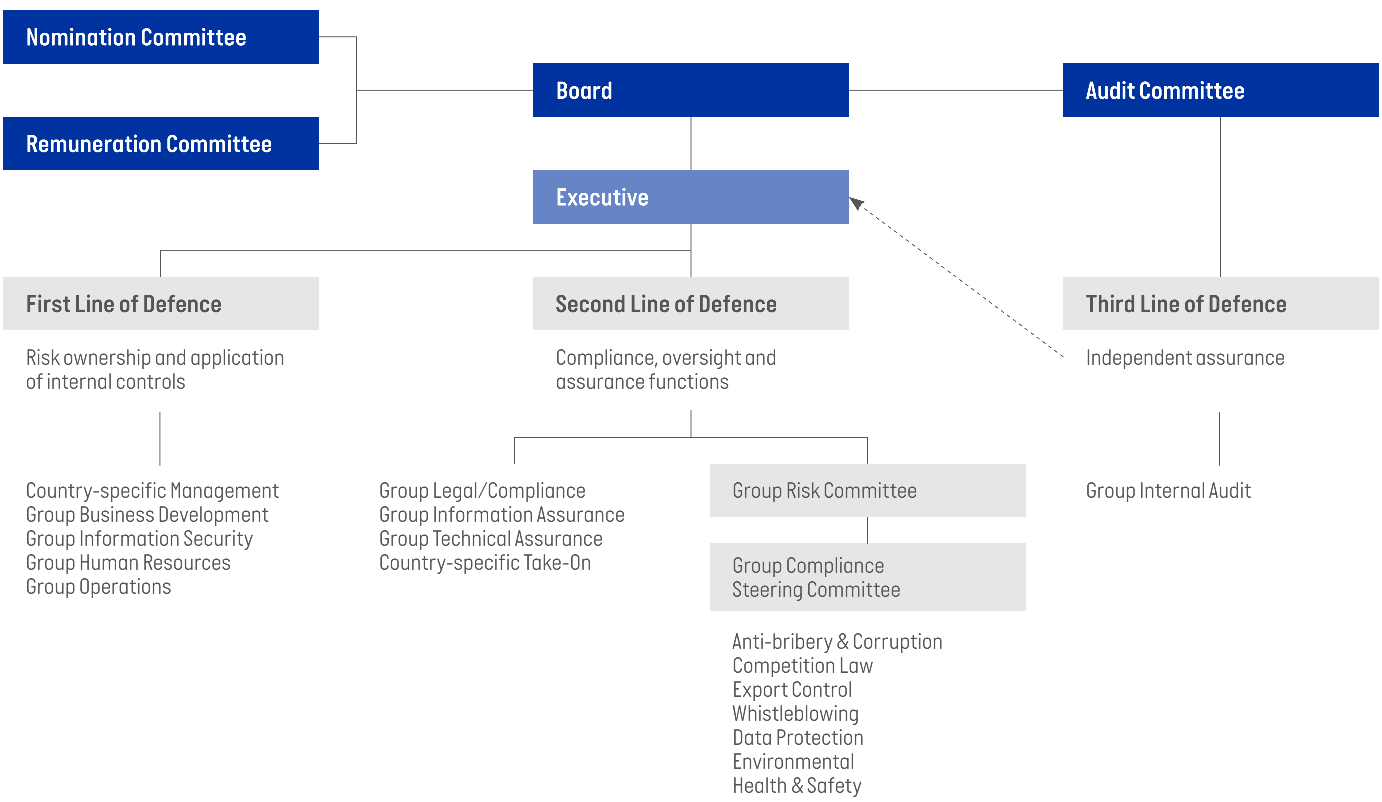
> "Identifying and assessing risk at the right level of our organisation allows us to empower our people, so they can provide the speed and flexibility our customers want."

Chris Webb
Group Chief Operating Officer

Risk management as a process to help maximise the chances of achieving our strategic objectives

Our risks:	STRATEGIC OBJECTIVES: To lead with and grow our Services business	To improve our Services productivity and enhance our competitiveness	To retain and maximise the relationship with our customers over the long term	To innovate our Services offerings to build future growth opportunities
1. Strategic Risk				
• Adverse technology change	●		●	●
• Inappropriate investment	●	●	●	
2. Contractual Risk				
• Underdelivery on contractual commitments	●		●	
• Ineffective international business strategies	●		●	
• Untested design and pricing structures	●		●	●
3. Infrastructure Risk				
• Cyber threat	●	●	●	●
• Systems outages	●	●	●	●
4. Financial Risk				
• Poor control of working capital		●		●
• Poor control of direct costs	●	●		
• Underinvestment in indirect costs	●	●	●	●
• UK's departure from EU	●		●	
5. People Risk				
• Poor staff recruitment and retention	●	●	●	●
• Inadequate succession planning	●			●

Risk Governance Model



Group Risk Log 2016 Heat Map

Principal risks	Principal impacts	Response to risk	Risk owner	Alert status
1 Strategic Risk • Technology change dramatically reducing customer demand for our service and product offerings • Not investing appropriately or over-investing in the wrong automation, self-service and remote tools, when compared to our competition	• Reduced margin • Excess operational staff • Contracts not renewed • Missed business opportunities	• 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	Chief Executive Officer	
2 Contractual Risk • Failure to deliver against contractual commitments for our Services business • Failure to deliver and manage our international business strategies effectively • Key empowered decision makers failing to implement appropriate designs and pricing structures	• Customer dissatisfaction • Financial penalties • Contract cancellations • Reputational damage • Reduced margins • Loss-making contracts • Reduced service and technical innovation	• Mandatory governance processes relating to bids, transitions and transformations • Board oversight of significant bids • Service management best practice • Established commercial governance processes embedded within the business opportunity and sales teams, including detailed cost analysis, risk-based decision-making and discussion of commercial summaries • Lessons learnt processes for complex transformations • Regular commercial 'deep dives' to manage service productivity improvements • Specialist international management team • Robust processes governing international business partners (subcontractors), before take-on and in-life, including alternate partners where applicable	Group Chief Operating Officer Head of International Country Managing Directors	

Principal risks	Principal impacts	Response to risk	Risk owner	Alert status
3 Infrastructure Risk • Hacking or virus affecting our networks and systems, leading to corruption or loss of business and personal data, or at a customer due to our fault, leading to the loss of customer data • Failure leading to unacceptably long or regular short outages of either internal or customer-facing systems	• Inability to deliver business services • Reputational damage • Customer dissatisfaction • Financial penalties • Contract cancellations	• Well-communicated Group-wide information security and virus protection policies • Specific inductions and training for staff working on customer sites and systems • Specific policies and procedures for staff working behind a customer's firewall • Ongoing and regular programme of external penetration testing • Policies ensuring Computacenter does not run customer applications or have access to customer data • Regular review of cyber security controls • All Group standard systems built and operated on high availability infrastructure, designed to accommodate failure of any single technical component • All centrally-hosted systems built and operated on high availability infrastructure, with multiple levels of redundancy • All centrally-hosted systems benefit from dual network connectivity into core datacenters designed to accommodate loss of network service • Standing agenda item for consideration at each meeting of the Group Risk Committee	Group Chief Information Officer Group Chief Operating Officer	↔
4 Financial Risk • 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 • Underinvesting in our indirect costs, particularly Sales, leading to missed opportunities and top line impact • Poor control of working capital • Letting our direct costs run out of control and not taking advantage of productivity and cost reduction opportunities	• 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	• 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 • 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 • Increased focus on direct delivery, reducing the level of 'free stock' in warehouses across the Group • Range of metrics employed to ensure we properly manage our direct costs and monitor productivity, including KPIs on staff availability, utilisation, cross-charge efficiency and contractor ratio • Significant direct costs managed centrally to retain control • Enhanced tooling and subsequent reduction in manual activity to deliver cost reductions	Group Finance Director Group Chief Commercial Officer Group Chief Operating Officer Country Managing Directors	↑
5 People Risk • Not recruiting and retaining the right calibre of staff across our customer-facing functions • Inadequate succession planning or insufficient depth within key senior executive positions	• Lack of adequate leadership • Customer dissatisfaction • Financial penalties • Contract cancellations • Reputational damage	• 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	Group Human Resources Director Chief Executive Officer	↔