

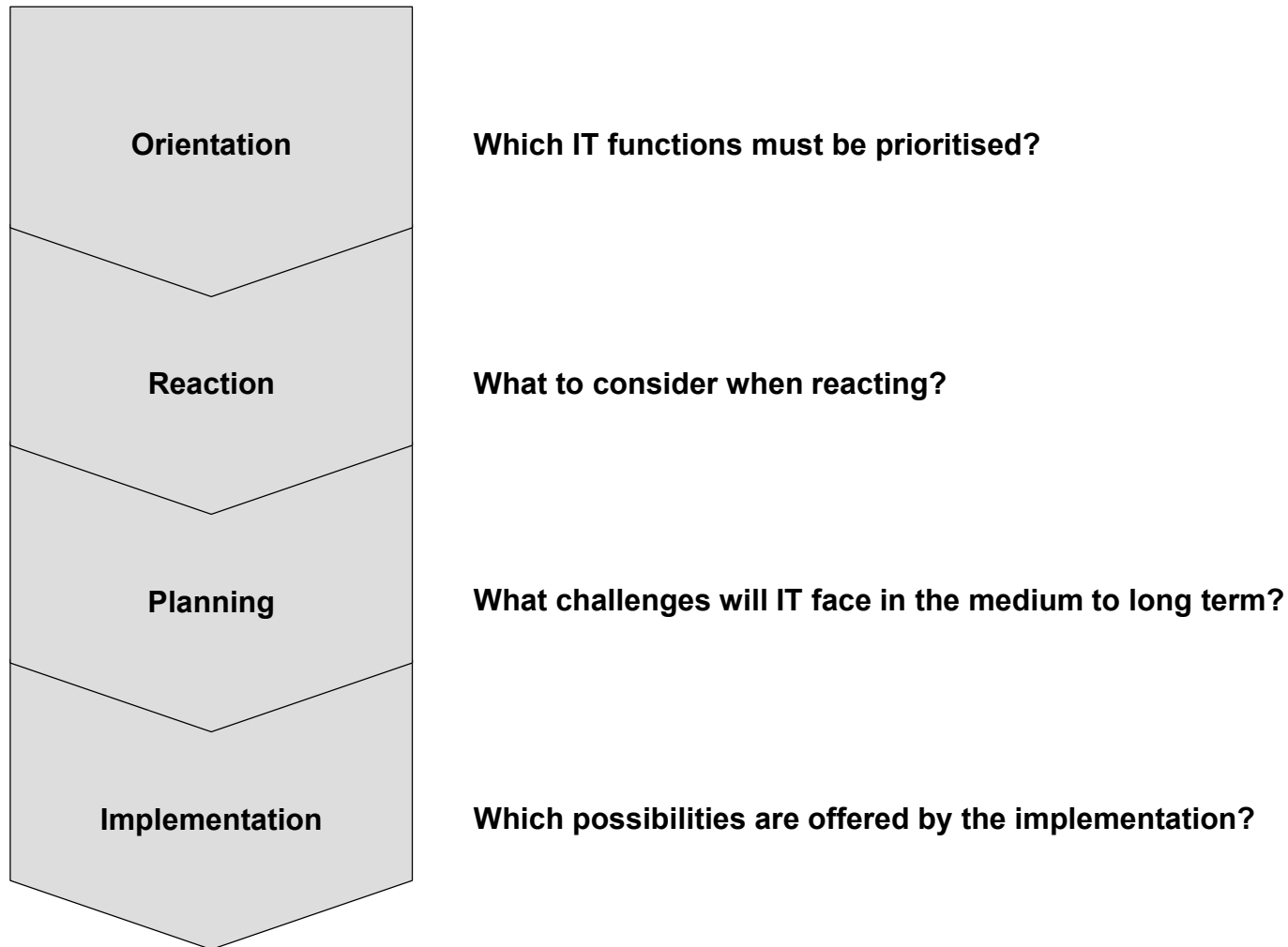
# **Competency in IT Management**

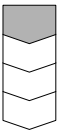
**Customer information  
on how to tackle the current challenges**

**Berlin, April 2020**

***The current situation requires not only a fast and flexible response from IT, but also a structured approach***

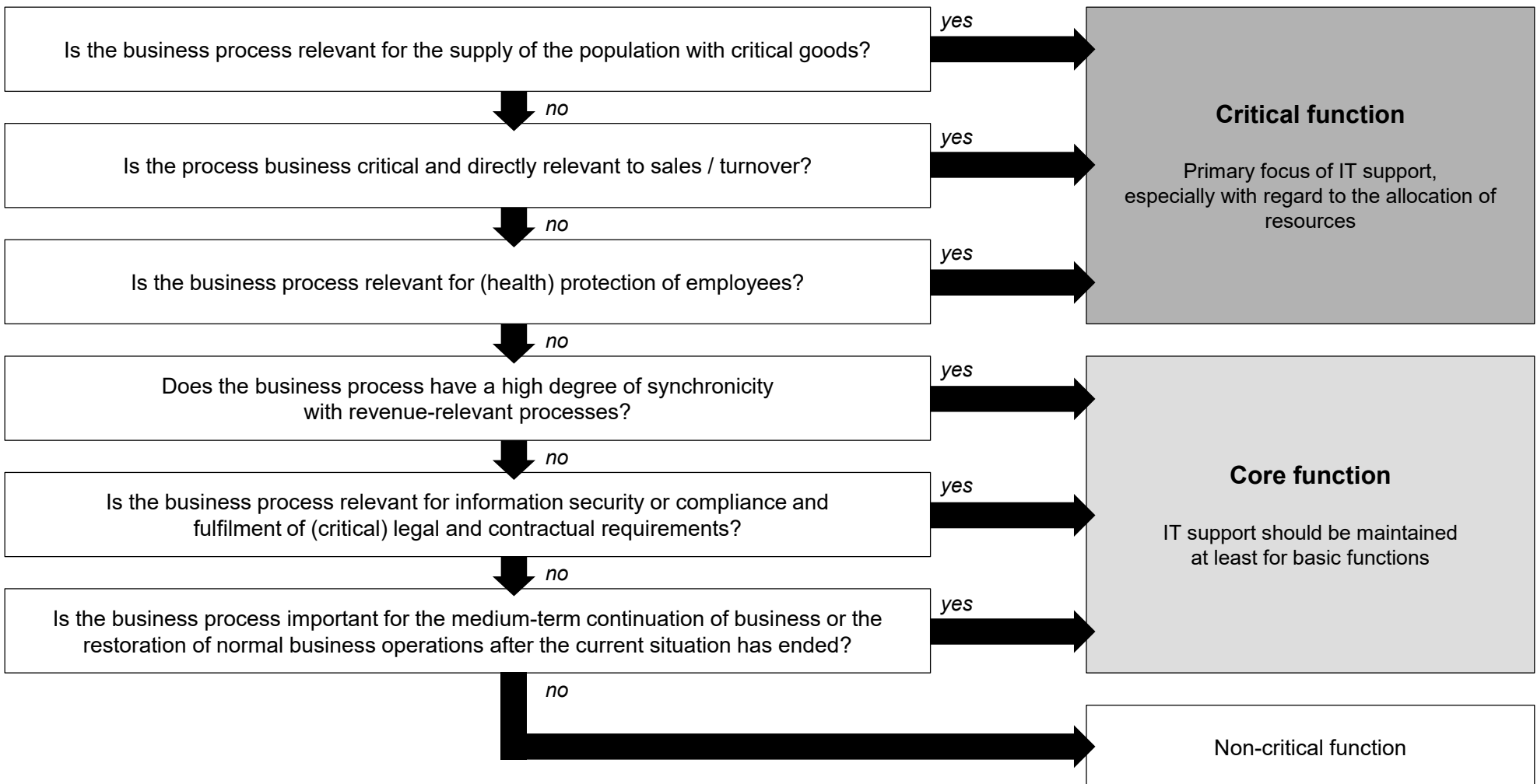
**APPROACH TO DEALING WITH IMPACTS OF CURRENT SITUATION**

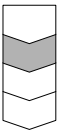




# ***IT support should be prioritised on the basis of a criteria-based assessment of business operations***

## **ORIENTATION**

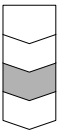




## ***IT is currently facing many challenges with ad-hoc solutions to ensure business operations – with important aspects to consider***

### **REACTION**

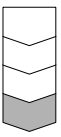
<b>Organisation</b>	<b>Data protection &amp; information security</b>	<b>Management &amp; governance</b>
<ul style="list-style-type: none"> <li>• Keep an overview of the ad hoc solutions so that you can “capture” them again later.</li> <li>• Provide uniform and joint solutions, e. g. for web conferences.</li> <li>• Consider the requirements of license agreements and data protection and adjust the resource situation (e.g. VPN accounts) dynamically.</li> <li>• What deadlines must be observed contractually, e. g. with ongoing acceptance / verifications?</li> <li>• Which contractual obligations exist, how can they be met?</li> <li>• Changes in production processes (e. g. “new” products such as protective masks) will also result in adjustment requirements for IT.</li> <li>• Use reduced / suspended production for patches and updates during “downtime”.</li> <li>• Create support opportunities for remote activities and collaboration solutions.</li> <li>• Always keep an eye on your costs!</li> </ul>	<ul style="list-style-type: none"> <li>• Protect “Use your own Device” (UYOD), for instance:               <ul style="list-style-type: none"> <li>– Container solutions (alternatively VPN)</li> <li>– Multi-factor authentication (soft token)</li> <li>– Use of web access for e-mail etc.</li> <li>– Patching of the end systems by employees and alternative measures</li> <li>– Dispose of confidential documents</li> </ul> </li> <li>• Ban the use of root / master accounts and keep the passwords etc. centrally.</li> <li>• Create awareness, e.g. with regard to attackers exploiting the situation (e. g. PDF coloring images with malware, sensitive content on photos from the home office, spying apps or even “smart speakers”).</li> <li>• Ensure privacy by default, including the disabling of functions in conference systems (e. g. “attention tracking”), setting up access restrictions for third parties.</li> <li>• Establish rules for desktop sharing and “digital factory tours”.</li> </ul>	<ul style="list-style-type: none"> <li>• Adapt the internal guidelines and policies (temporarily) to the changed situation (e.g. coordination with employees)</li> <li>• Decentralized and asynchronous cooperation requires an increased level of trust and understanding, both from the management and the employees, and fixed structures are an enormous help in this respect.</li> <li>• Create motivation and exchange opportunities for the employees, e. g. through “virtual coffee / tea breaks”.</li> <li>• Inform employees regularly through open communication and joint “pick-up points”.</li> <li>• Avoid the accumulation of knowledge in individual employees.</li> <li>• Carry out continuous personnel and resource planning and build up a personnel reserve if necessary.</li> <li>• Set up personnel substitution rules and ensure that substitutes have the appropriate knowledge and information (including access rights).</li> </ul>



***The current situation will continue for some time – therefore it is all the more important to anticipate the challenges that will follow***

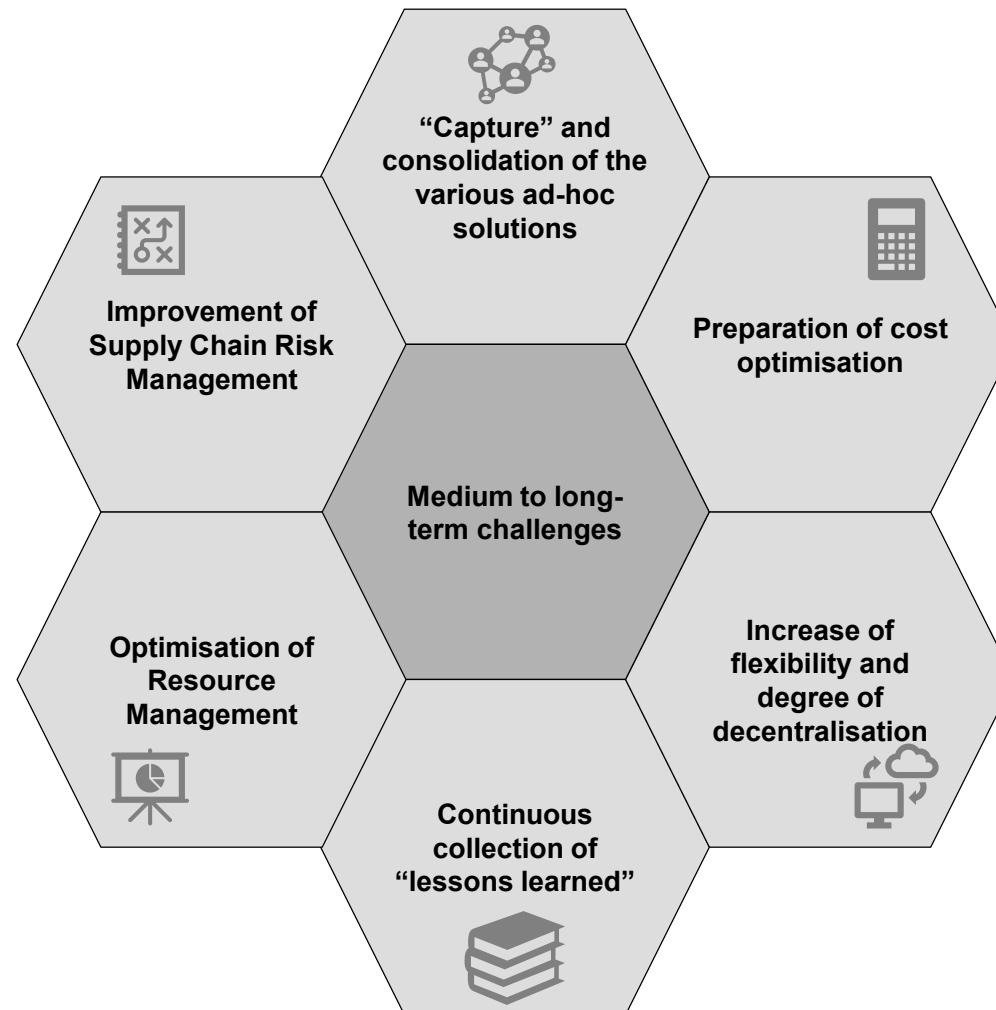
**PLANNING**





# ***Already now, first steps can be undertaken to prepare the IT for the upcoming time***

## **IMPLEMENTATION**



***Please do not hesitate to contact us for further information***

**CONTACT INFORMATION**

**Roger Sparks**

Managing Director UK

Mobile +44 78 87950705

Email [sparks@lexta.com](mailto:sparks@lexta.com)

LEXTA UK Limited

Friary Court, 13-21 High Street

GU1 3DL Guildford, Surrey

United Kingdom

**<https://www.lexta.com>**

**Frank Baumann**

Managing Director Germany

Mobile +49 172 7606738

Email [baumann@lexta.com](mailto:baumann@lexta.com)

LEXTA GmbH

Dorotheenstraße 37

10117 Berlin

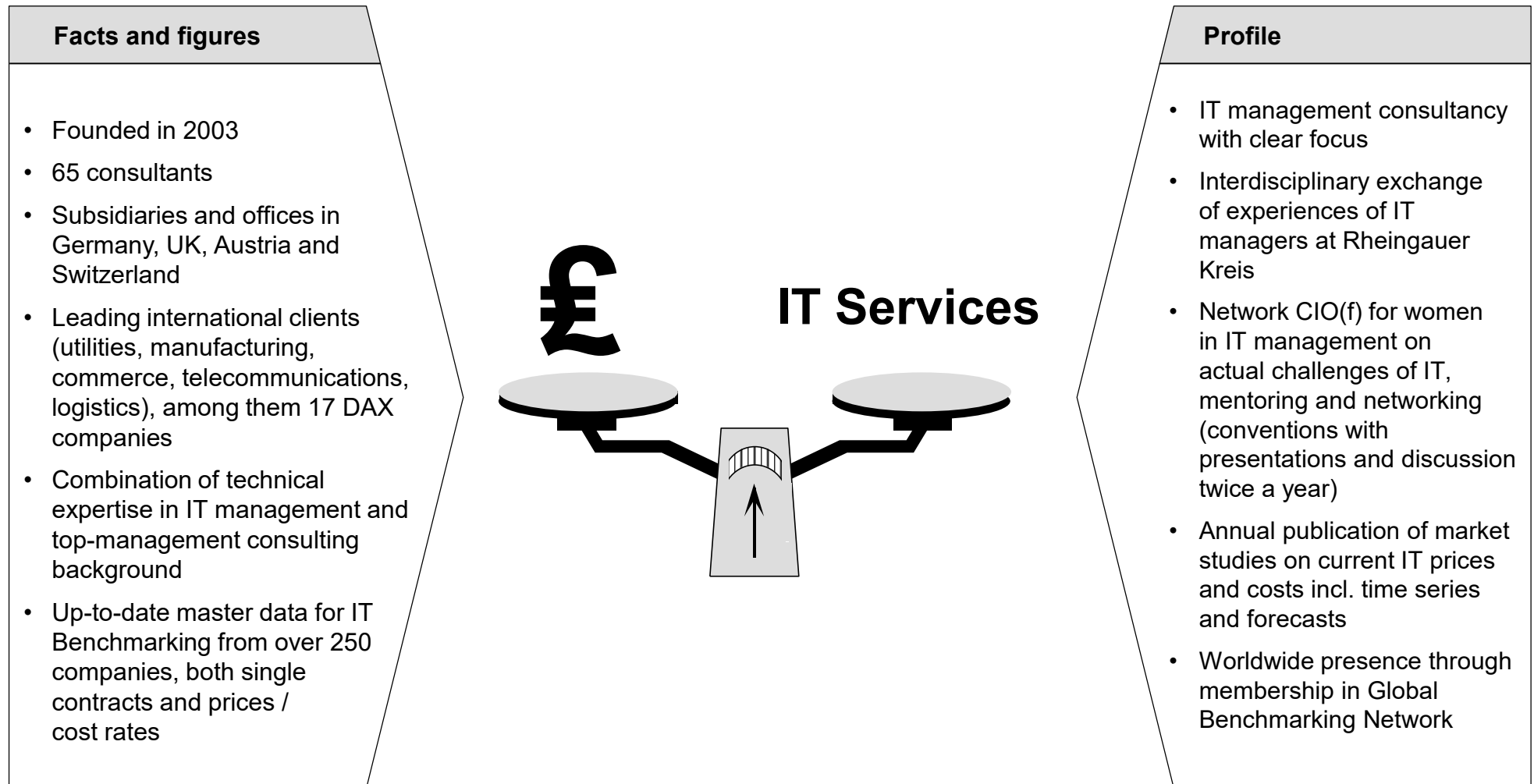
Germany

# ABOUT LEXTA



# **LEXTA is one of Europe's leading IT consultancies focussed on the competitiveness of IT services**

## **OVERVIEW LEXTA CONSULTANTS GROUP**



# ***LEXTA offers a performance portfolio based on IT benchmarking that covers all key issues in IT management***

## **LEXTA PERFORMANCE PORTFOLIO**

