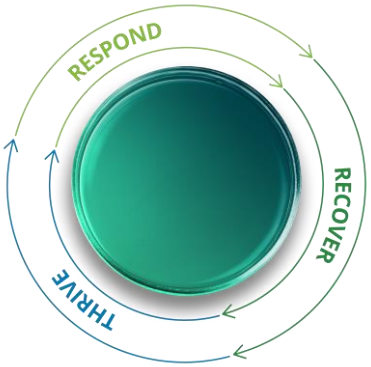
Deloitte.
Legal



Accelerate digitization to increase resilience

A global COVID-19 response for legal leaders

Current digitization strategies typically focus on *increasing* productivity of a company. *Maintaining* productivity is, however, equally important as the COVID-19 pandemic demonstrates. A robust technical infrastructure and end-to-end digital processes ("paper-less") are key elements to safeguard productivity during disastrous events. First-response actions such as implementing business continuity plans and stabilization of business operations should be accompanied by proactive measures: companies should rethink and accelerate their digitization strategy to *increase resilience and optimize business processes* at the same time. Contractual arrangements with IT service providers should be revisited, data privacy and security topics as well as industry-specific regulations must be kept in mind. Although companies are now busy responding to the COVID-19 challenge, we will soon face a recovery phase that will once again show the importance of a holistic and sustainable digitization strategy. Using "lessons learned" is key to prepare for and thrive in the future.

Maintain productivity while keeping it safe and economically sustainable

Ensuring business continuity is one of the highest priorities for every company, and in these days, many may be forced to cut costs. If they do so, however, they should not lose sight of the long-term implications of the crisis. Once the situation has been stabilized, companies must rethink their digitization strategy and put measures in place that establish sustainability for the future challenges to come.

- Business continuity
- Cost cutting
- Rethink digitization strategy
- Establish sustainability

Respond – Recover – Thrive

Timely response to the new situation is key, by **proactively tackling pressing issues**.

Development of the means to **adapt existing processes and strategies** is imperative, as well as the identification of digitization potentials to increase resilience and cut costs at the same time.

Implementation of those new processes and strategies, and **establishment of sustainability** are achieved by assessing (the risk) of future crises.

Actions to consider

Respond

Companies can respond through:

- Discussion with software providers regarding **business continuity and scalability**. The provider contract regarding service reduction, up- and down-scaling (e.g., force majeure clause or statutory law), and how to compensate any deterioration of the service quality should be considered. SLAs should be monitored closely, with penalties o and enforce service level credits or penalties.
- **Adaptation of the costs of provider** by identifying and exploiting savings potential, e.g., pausing/ terminating services or switching to pay-per-use; and discussion of "creative" solutions, e.g., longer fixed terms for reduced fees.
- Investment in infrastructure for **remote working**: e.g., obtaining more bandwidth, hardware, cloud capacity etc., and ensuring that the required licenses for remote work are available.
- Keeping the **data protection** organization up and running, and ensuring **data privacy & security**. Essential compliance processes should be working.

Recover

Once recover commences, companies should consider:

- **Evaluating and updating** their and their providers' **business continuity plans**. Renegotiation may be necessary, and the provider could distribute, where possible, the costs among all its customers.
- **Rethinking and accelerating their digitization strategy**, with the focus on resilience and scalability of business critical functions in case of disasters. In those events, providers are likely to be confronted with numerous similar requests, so it would be prudent to prioritize good-value-for-effort and quickly-implementable measures.
- **Developing new remote working concepts**, such as the provision of sufficient soft- and hardware. Training the workforce, and preparing manuals and Q&As, may help to solve IT problems fast. It would also be useful to perform stress tests to assess the systems resilience, and agreeing future disaster recovery protocols with the workforce.
- Defining compliance and business critical **data privacy & security** topics and measures for different crises scenarios.

Thrive

Once able to thrive again, companies should consider:

- **Implementing a digitization strategy** by procuring the required technology. Contracts protect the company's interests (scalability at all times, sufficient SLAs/penalties, force majeure clauses, termination rights, exit support etc.). Processes should be digitized, but data security & privacy standards should be maintained, and industry specific regulations (e.g. EBA Guidelines) should be monitored.
- **Preparing for the future and establishing sustainability** by (risk) assessing the organization on future disasters, and testing the preparedness of the organization and technology based on different potential scenarios. Issues should be identified and measures defined to optimize preparedness.
- Implementing and testing guidelines, including measures and reporting processes, within the **data protection organization** and **IT department** to optimize the response to different crisis scenarios.

Contact:

Dr. Till Contzen
Partner, Deloitte Legal Germany
+49 69 719188439
tcontzen@deloitte.de