

RESULTS

Thank you for completing the IDC 'Is your infrastructure future-ready?' quiz sponsored by Dell and Intel. The economic benefits of being future ready are clear — increased future readiness corresponds to better business outcomes.




Organizations don't have to be at the top of the future-readiness scale to enjoy benefits; data from a number of IDC Converged Infrastructure and Cloud studies have shown that organizations can obtain benefits by moving to the next stage of future readiness regardless of where you start. Organizations that improve their "future readiness" consistently improve their time to market with new products and services, increase business agility, employee productivity and even improved innovation.

The more that an IT organization is future ready, the more that they enjoy significant business advantages over their competition, including:

- Faster time to market for new products and services, which allow them to better capture competitive advantages
- Superior business agility and flexibility, enabling them to anticipate and respond quickly to changes in the market, mitigate threats, and capture opportunities
- Increased employee productivity, allowing them to optimize business processes and reduce costs while increasing output
- Enhanced customer experience to deliver more reliable, intuitive and better performing services to employees, partners, and customers
- Innovation, which enables them to move resources and operations into new business areas
- More efficient IT operations, helping reduce costs while creating a more scalable infrastructure
- Enablement of mobile operations to deliver a full range of business applications

The quiz was designed to help establish your organization's readiness to cope with the evolving demands that businesses place on IT infrastructure, both today and into the future.

We looked at the following key areas:

-  IT and the Business
-  IT Service Delivery
-  IT Infrastructure Technology

Based on your responses, we would classify your overall IT Infrastructure Future Readiness as:

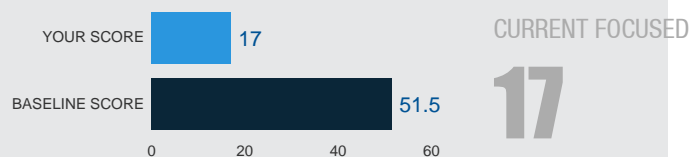
CURRENT FOCUSED

Based on your responses, we would classify your overall IT Infrastructure Future Readiness as:

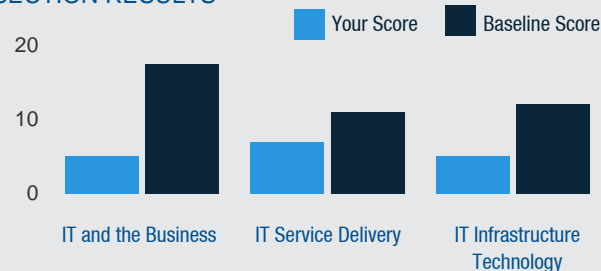
You have been rated Current-Focused, and are doing pretty well on the future readiness of your IT infrastructure. But even for those doing well, future readiness is an ongoing journey, and you can still see improvements in business outcomes from increasing your future readiness. As technologies, business practices, and market demands change over time, the concept of future readiness will also evolve. To maintain future readiness, organizations can't become complacent —think of future readiness as an ongoing journey and stay nimble, adaptable, and innovative to maintain their competitive edge. You can drive business results by choosing to focus on improving the specific aspects of IT Future Readiness landscape that we've highlighted for you:

• **IT and the Business** • **IT Service Delivery** • **IT Infrastructure Technology**

OVERALL READINESS



SECTION RESULTS



IT and the Business

According to your responses in this section, your organisation's Business Effectiveness & IT Capability TechFitness is **reactive**

How to get ahead?

- IT should not be considered a cost centre in organisations. IT should be considered crucial in achieving a competitive advantage. Currently, only 56% of European organisations believe that their IT makes an important contribution to business objectives.
- Ensure compliance risks are understood throughout the business. Regulatory compliance is increasingly more prescriptive and officials more fervent in what they expect from organisation's compliance programs. Regulatory compliance should be integrated into IT strategies at the development stage with a major focus on security.
- Understand the business processes and requirements before attempting to automate document workflow. Digitised business

workflows have been adopted, or plan to be adopted by three quarters of organisations interviewed, however to successfully deploy an automated document workflow you need a full understanding of business rules and procedures before looking for the right solution.

- Adopt telecom expense management to manage costs. 86% of organisations have adopted the use of mobile devices, the cost of running these are very much driven by individual usage. The need to control the cost of these devices is therefore of critical importance. Around one-third of companies are adopting telecom expense management to manage costs associated with mobile device usage.
- Implement print device usage and reporting facilities. Controlling who can print what, and where, leads to considerable cost savings, as well as other benefits such as enhanced privacy and security, reducing legal and business risk. IDC research shows that 26% of European SMBs have printing device usage and reporting facilities in place today, while 24% have implemented printing device security and ID solutions.



IT Service Delivery

According to your responses in this section, your organisation's IT Security TechFitness is: **reactive**

How to get ahead?

- Security is a business function that needs to be incorporated into the way you do business. Security should be built by design rather than as a bolt on afterthought. 93% of IT users view the improvement of security for existing employees and devices as their highest security priority.
- Create secure, protected workspaces within central servers to eliminate risks in the deployment of mobile devices. Mobile employees drive the need for secure access to data, however data loss prevention is a serious and recurring problem for almost all organisations. Sensitive data protection is the second most important business objective for businesses (60%).
- Restrict printing to 'document owner present' minimises sensitive data loss through unauthorised persons reading/copying documents. Loss of data or unauthorised copying and reading of sensitive documents can be a serious business risk and open the door to legal action. Around 30% of European SMBs have such solutions in place today.
- Control your mobile devices through Mobile Device Management (MDM) software. MDM allows network administrators to secure mobile devices regardless of connection. The management of mobile computing should be based on the principle of isolation of transactions so that any malware incursion can be isolated, examined, and then discarded. Other features include the encryption of files, authentication and access privileges, locking down applications, and validating security identification. 62% of companies below 1000 employees have adopted, or will adopt within the next 24 months, MDM.



IT Infrastructure Technology

According to your responses in this section, your organisation's Cloud TechFitness is: **reactive**

How to get ahead?

- Focus on the architecture and planning. Cloud has the potential to turn any mobile device into a supercomputer, providing access to processing power as needed to analyse virtually any type of information required. However, performance issues can affect cloud computing efforts; this is caused by cloud-based apps being widely distributed, with the data far away from the application logic. Unless careful planning has gone into the design of the system, latency and reliability may become major issues.
- Inform, educate, and control users over their file sharing activities. Although Cloud storage facilitates collaboration, mobile working, and can be more cost-effective, it is also in high demand from end-users and not having a solution in place leads to increased 'shadow IT' as users adopt consumer solutions. This in turn may lead to increased business risk through lack of control. In the latest IDC survey around 20% of organisations had implemented a cloud-based file sharing solution – mostly to a restricted set of users.
- Evaluate your data security needs. Preferences for data location and data security are often based on personal preference and misinformation. Consult with your local data privacy office to understand the actual requirements for certain data types, such as financial information, customer information, employee information, and personal identifiable information.
- Audit your organisation's printing infrastructure. Consider device type (printer, MFP, toner, inkjet), brand, and age of devices. Evaluate the requirements of your internal customers – and, potentially, of external partners and other stakeholders that may need to print at corporate locations – including document types and output features. Today, 39% of European companies utilise cloud-printing, potentially benefitting from increased productivity and flexibility, while reducing the need for local infrastructure (fewer PCs deployed).
- Evaluate your existing level of maturity for cloud services to begin vendor qualification process. 70% of surveyed organisations stated that improving IT security due to Cloud/SaaS usage was a very or extremely important part of strategy for the upcoming 12 months. Investment in the correct training and development is needed for the enterprise staff to ensure they understand how to operate securely in a cloud environment.