

Survey Report:

The State of ITSM in the COVID-19 Pandemic



ManageEngine
ServiceDesk Plus

Survey Report: The State of ITSM in the COVID-19 Pandemic

The COVID-19 crisis hit the world hard in both social and business terms. From a business perspective, it required many changes – from the products and services offered (and the way that they’re produced, marketed, and sold) to how employees work. And, given the nature of modern business, most changes had an impact on IT operations, including the corporate IT support capability.

To understand how well IT departments coped during the early days of the COVID-19 crisis and which factors influenced success, ManageEngine surveyed 519 IT professionals across a range of topics. The results are contained within this report. ManageEngine would like to acknowledge the contribution of Stephen Mann, Principal Analyst at itsm.tools in drafting this survey report.



Survey Findings

The ManageEngine survey asked 15 questions across 5 areas:

- The impact of employee remote working
- Financial and asset management implications
- Security and governance issues
- Third-party services and technology assistance
- Business continuity success levels.

The findings from all 15 questions are reported in this paper along with identified correlations between different questions and their answers. There are, of course, numerous possible question pairs within a 15-question survey. So, a sample of 45 pairs was examined with the observed correlations included within each question section.



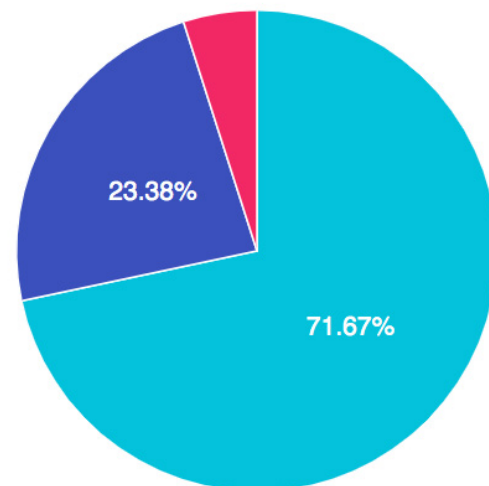
The impact of employee remote working

The mass, and rapid, migration of employees from office-based to remote – usually home – working provided one of the [biggest impacts on IT departments and IT service desks](#) in particular. While it was a difficult logistical exercise in its own right – getting a significant number of employees working productively remotely – the fact that service desk analysts could also be homeworkers, or missing colleagues due to illness, added an extra layer of complexity. The ability of IT organizations to deal with the new way of working, and remote support, is addressed in questions 1 through 3.

Q1

Do you think IT service management is effective when done remotely?

The majority of survey respondents (72%) think that [IT service management](#) continues to be effective in remote scenarios. Which could involve remote end users, remote IT personnel, or both. With only 5% of respondents thinking that IT service management is less effective when done remotely. Hopefully, these views have been supported, or will be later validated, by similar or better CSAT results being achieved during the crisis versus any previous office-based surveys.



- Yes, it can be effective when it's done remotely
- Yes, it can be effective, but only when it's partially remote
- No, it's ineffective when it's done remotely

Unsurprisingly, the “ITSM is ineffective when it’s done remotely” option is correlated with “Unable to meet the challenge” (from question 15 – on the overall level of IT service desk success) and “We are unsatisfied. We want better control and plan to move it back in-house” (from question 10 – on the use of managed service providers). It’s also correlated with both not having business continuity plans and plans that weren’t able to help sufficiently during the pandemic (question 13).

Whereas, and again unsurprisingly, “Yes, it can be effective when it’s done remotely” is correlated with “Yes, definitely” (from question 6 – on the value of IT being better-recognized post-crisis).

Q2

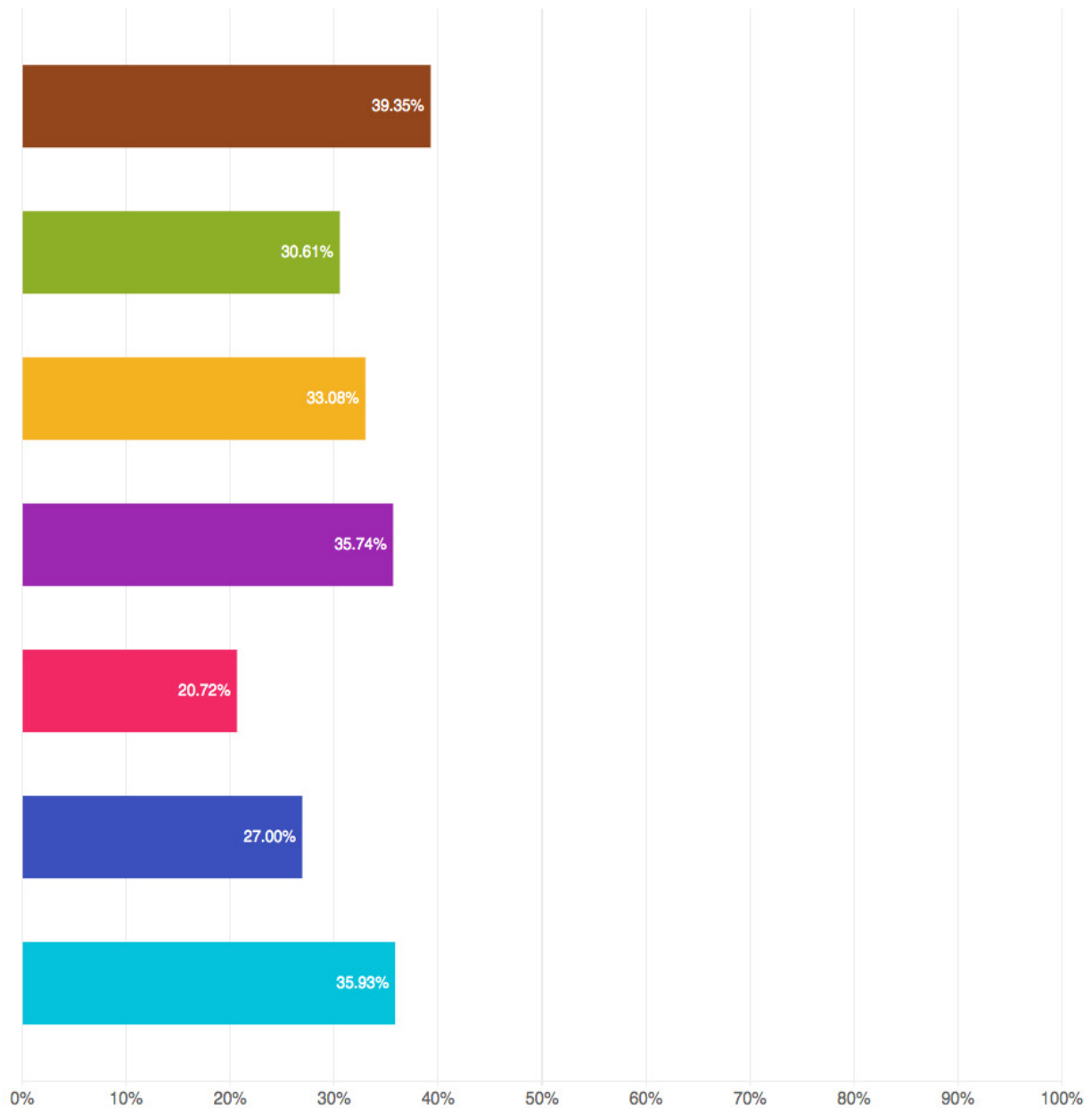
What do you think is the greatest challenge in offering remote IT support?

The survey found that not all remote IT support challenges are “born equal.” Interestingly, two of the most commonly touted issues during the COVID-19 crisis had the lowest traction in the survey:

- VPN or employee connectivity issues (in fifth place), where thankfully the uptake of cloud-based services negated the need for VPN use in many instances.
- An increase in service desk tickets (in seventh, and last, place). Here, while there might have been an initial influx of additional tickets related to equipment requests and teething issues, for many IT departments the increased ticket level dropped again once employees were settled into their new working environments.

Instead, the most commonly found IT support challenges related to training and knowledge management – where limitations could adversely affect both end users and IT personnel in the support of them – and the security issues connected to employees working remotely.

The first of these highlights what’s a continued challenge for IT departments – [effective knowledge management](#). With this compounded by the use of new technological capabilities – such as collaboration tools for end users and remote support tools for service desk analysts – which might have required the creation of new knowledge articles during a time unprecedented IT service desk pressure.



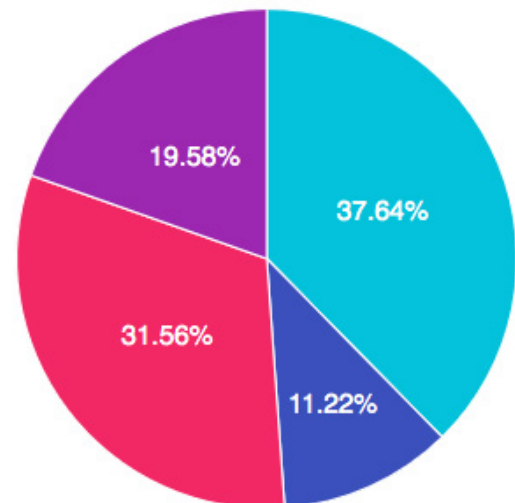
- Managing IT assets
- Lack of appropriate technology
- Too many L1 tickets (more than usual)
- Securing company and client data in a distributed network
- Communication and collaboration
- VPN issues: configuration, scalability, and troubleshooting
- User training and knowledge management

Did your bring your own device (BYOD) policies hold up in the transition from office to remote IT support?

The use of personal devices by employees for work purposes is nothing new, with BYOD challenges, approaches, and policies now well over a decade old. Such policies could range from employees being able to use personal devices for work (or not, especially in highly-regulated work environments), through the corporate support of these personal devices, to the organization financially contributing to personal devices and/or providing corporate purchasing deals and discounts.

In the case of the impact of the COVID-19 crisis, the key related point is that employees might need to use their personal PCs and mobile devices while working at home. For example, because of corporate homeworking equipment sourcing difficulties, poor signal quality for corporate mobile devices, or the prohibitive cost of supplying additional equipment. They might have also needed to personally purchase new IT equipment to stay productive. Then there's the expectation and need for IT to support the setup and ongoing use of these personal devices, apps, and even cloud services.

One of the most unexpected survey findings is that more than half of organizations had no BYOD policy. So, there were no agreed corporate rules related to personal IT use and security, and the support of personal devices, that could be applied to help with the continued productivity of employees in their new remote working environments.



- Yes, it held up well
- No, it did not help us much
- We do not have a BYOD policy in place
- We don't have a BYOD policy, but the pandemic experience is sure to expedite things

As expected, the availability of relevant BYOD policies was of help during the pandemic. For example, the “BYOD policies holding up well” option correlated with both “We did a great job despite some hiccups” (from question 15), “Yes, definitely” (from question 6), and “Yes, we had good plans to fall back on” (from question 13 – on business continuity plans).

Financial and asset management

In financial and asset management terms, there's both what happened during the crisis and what will happen post-crisis to consider. For example, there's the ongoing need to support homeworking better and the need to have better contingency measures in place.

Plus, the commercial impact of the COVID-19 crisis will be felt for the rest of 2020 and beyond – where many employees have lost jobs, many businesses have sadly gone under (and more continue to do so), and for those that survive the next 12 months will likely be a struggle. From continuing to operate in an “unnatural environment” to coping with increased competition as the companies that remain fight over what will be a lower level of spending.



Q4

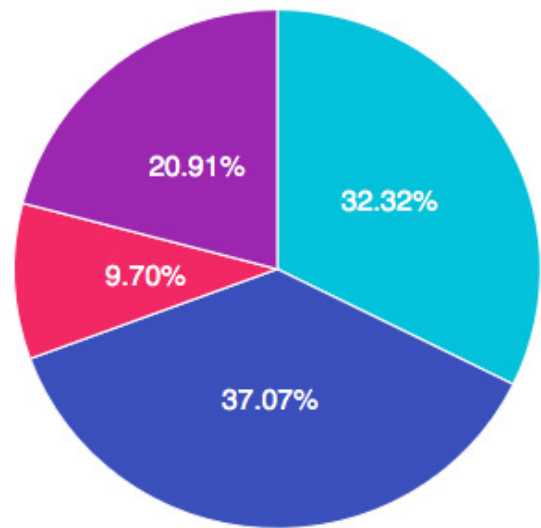
If your asset procurement policy was geared toward desktops and on-premises servers, are there any plans to rework the policies to accommodate mobile-capable assets like laptops, tablets, and smartphones?

The survey found a mix of corporate stances on how best to equip employees with suitable technology. Only 32% of organizations were already providing mobile-capable assets before the crisis. Which might have been influenced in part by the organization's industry vertical and the level of what have traditionally been called “knowledge workers.”

After the challenges of early 2020, close to half of organizations will now look to provide more mobile-capable assets to employees. And only 21% of organizations will not change their IT procurement policies to provide greater mobility and flexibility.

The provision of mobile-capable assets definitely helped to handle the migration of employees to home-based working. The “We used mobile-capable assets from the beginning” option correlated with “We did a great job despite some hiccups” (from question 15).

Oddly, though, in the same pairing, the organizations that were “Unable to meet the challenge” are most likely to be “Not currently planning any change in procurement policies.” This could, of course, be due to a known financial limitation and an inability to change – and the “Not currently planning any change in procurement policies” option also correlated with “No, things will not change” (from question 6).

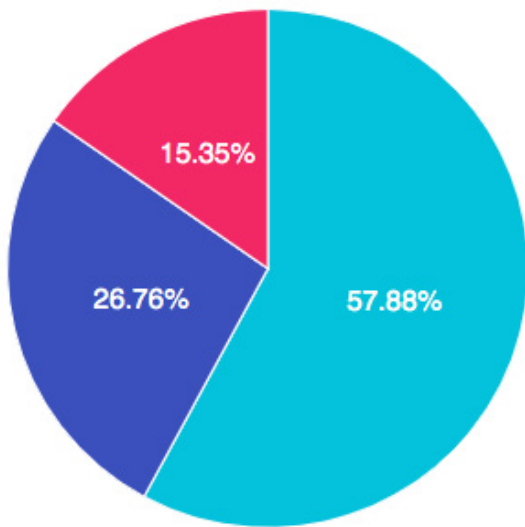


- No, we used mobile-capable assets from the beginning
- Yes, we are planning to have a mix of mobile-capable assets and on-premises assets
- Yes, we are planning to procure only mobile-capable assets from now on
- No, we are not currently planning any change in procurement policies

Q5

Were you equipped with remote support tools, VPN licenses, and other necessary applications before your employees went remote in response to COVID-19?

There’s good news related to organizations having the required technology to support remote workers before the crisis – most organizations (85%) already had the right remote-support equipment or were quickly able to get it. Only 15.4% of organizations still didn’t have what they needed well into the crisis.



- Yes, we were sufficiently equipped
- No, but we were able to acquire what we need to get through
- We're still under-equipped

As expected, those who were underequipped struggled during the pandemic. For example, the “We’re still under-equipped” option is correlated with “Unable to meet the challenge” (from question 15). This didn’t only apply to internal IT service desks, it also applied in MSP scenarios – with there is also a correlation with “We are unsatisfied. We want better control and plan to move it back in-house” (from question 10).

Q6

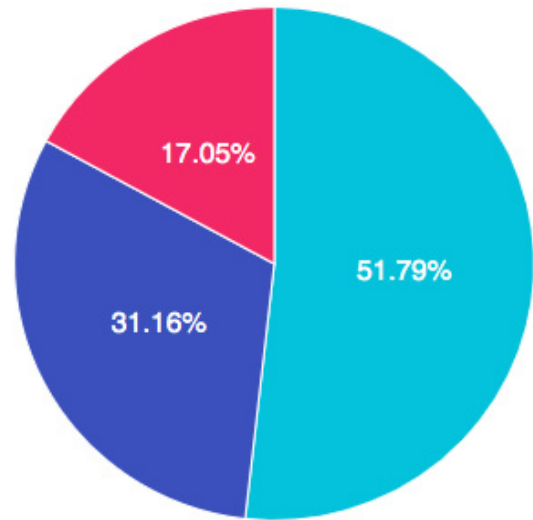
Do you think IT will be taken more seriously in terms of budgets, salaries, and recognition of effort after all this?

There’s no doubt that the efforts and hard work of IT support staff, in particular, were recognized as playing a key role in dealing with the crisis and the challenges it brought with it. In a similar way to how healthcare workers, supermarket staff, and delivery personnel were all lauded for the vital contributions they respectively made during the crisis, IT staff were usually more appreciated than previously. But will this appreciation continue post-crisis, including in reward and recognition terms?

The survey found that 83% of respondents think that IT will be better viewed and treated post-crisis. Although 31% of these expect the greater appreciation only to be short term. It would be great if IT support staff, in particular, are valued and recompensed more going forward; but if only half of IT personnel think they will be valued more, then it doesn’t bode well. Especially in light of the expected financial challenges post-crisis.

Unsurprisingly, the “No, things will not change” option is correlated with “Unable to meet the challenge” (from question 15). After all, why would things change if the IT service desk didn’t perform well?

- Yes, definitely
- Short term, yes. Long term, no
- No, things will not change



Security and governance issues

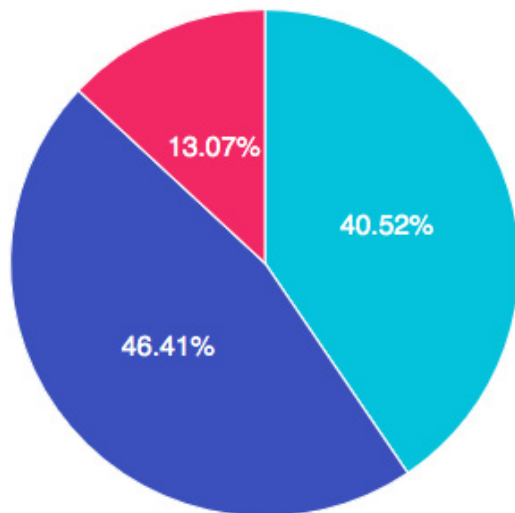
At the outset of the crisis, the need for business continuity was paramount – as organizations reorganized and reinvented to remain operational while isolation-based legislation hit business-as-usual both inside and outside the office walls. The new ways of working needed to be effected immediately, with those responsible for security and governance in a difficult position – in balancing the need to protect the organization (as it changed) while also protecting the ongoing ability for it to “be in business.”

Q7

Is your organization equipped to tackle the increase in security and privacy concerns with most employees working outside the office now?

The speed of change and the stark contrast between traditional office-based working and the new remote working environments is evident in the survey responses – with only 40% of organizations viewed as being equipped to tackle the increase in security and privacy concerns related to employees working outside the office.

- Yes, we are confident in our security and privacy measures
- Yes, but we could do better to strengthen security and privacy
- No, we are under-equipped to handle it



Unsurprisingly, the “No, we are under-equipped to handle it” option is correlated with “Unable to meet the challenge” (from question 15). Conversely, for those organizations that use, and are satisfied with, MSP services are more likely to be “confident in our security and privacy measures.” Business continuity plans also played their part, with the “Yes, we are confident in our security and privacy measures” option correlated with “Yes, we had good plans to fall back on” (from question 13).

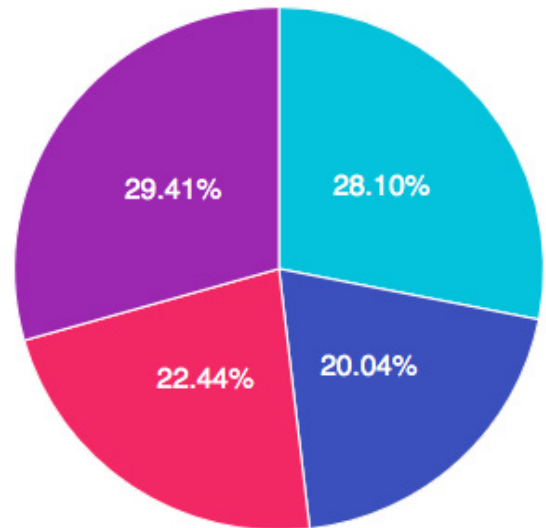
Q8

With the ongoing work-from-home situation, is there an increase in shadow IT in your organization?

Shadow IT can be a range of things within an organization. From employees “unofficially” using personal devices, apps, and cloud services for work purposes through to departments “doing their own thing” in procuring potentially business-critical applications and services. Where the first thing the IT department knows about it is when there’s an issue and they’re expected to support it.

While the [implementation of BYOD policies](#) can address many of the risks associated with the first of these, the latter can cause an organization considerable harm – from business interruptions to data loss, potentially resulting in revenue loss, penalties, and brand damage.

While nearly one-third of respondents were unsure of any adverse effects from shadow IT, one-fifth of respondents reported that they faced “impactful services and applications” during the already difficult times.



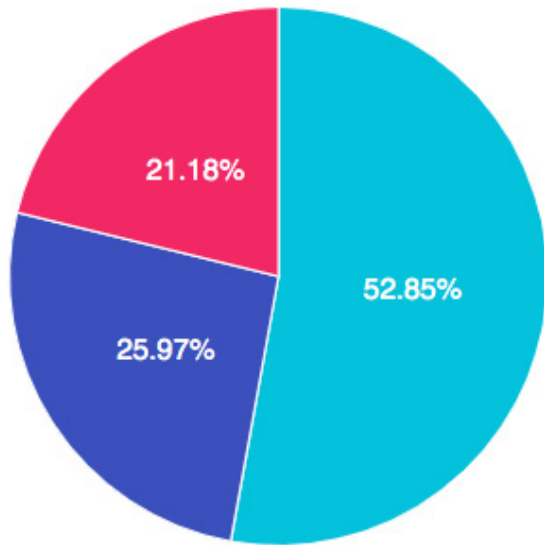
- Yes, but nothing unexpected or impactful
- Yes, we're facing impactful services and applications
- No, we keep it quite strict
- Not sure

Q9

How well did your transition to the cloud pay off for your organization's business continuity?

Of the organizations that had moved much of their IT to the cloud, two-thirds felt that this had helped them considerably during the COVID-19 crisis. However, the remaining third felt that it didn't help as much as they'd expected. This would, of course, have likely been dependent on which services had been migrated (to the cloud). In particular, those used for personal productivity – such as email and Office – and key business applications, such that employees could work remotely without the need for VPN connectivity.

For one-fifth of organizations, the impact of the pandemic has caused them to reconsider, and regret their delay in, moving key services to the cloud.



- It helped a lot
- It didn't help as much as expected
- We did not move to the cloud, and that choice has cost us dearly

As expected, the use of cloud services was an important factor for [ITSM success](#) during the pandemic. For example, “Cloud helped a lot” is correlated with both “We did a great job despite some hiccups” (from question 15) and “Yes, definitely” (from question 6). For those organizations that are happy with their MSP services, there was a higher adoption level of cloud which “helped a lot.”

Third-party services and technology assistance

For most corporate IT service providers, there are a variety of options available to them to help improve IT service delivery and support from a quality or cost perspective, or both. For example, outsourcing certain IT service management capabilities to a third-party, employing now-expected time and cost-saving technology, or investing in newer technologies such as artificial intelligence (AI)-based capabilities for “better, faster, cheaper” solutions.

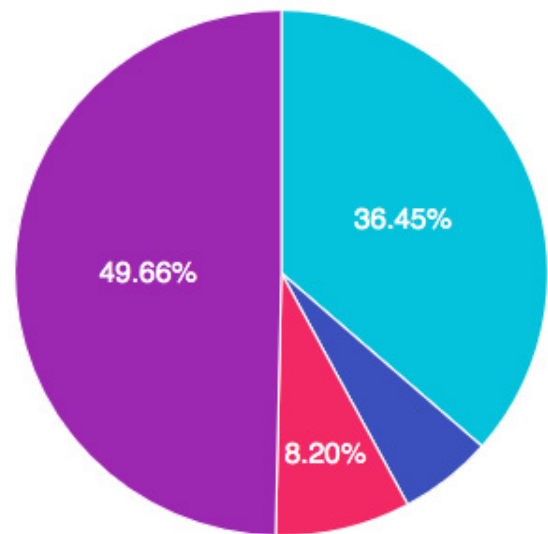


Q10

If you outsourced your ITSM operations to a managed service provider (MSP), how satisfied are you with the performance of your MSP during the pandemic?

It should be noted that only roughly 80% of survey respondents answered this question; but, even so, it shows a high degree of MSP use within the survey sample at circa 40% of organizations. Of these, over one-quarter (28%) were unhappy with their MSP's performance during the pandemic. With 17% so dissatisfied that they plan to bring their outsourced services back in house post-crisis.

Unsurprisingly, the “We are satisfied” option is correlated with “We did a great job despite some hiccups” (from question 15). As is the “We do not avail the service of an MSP” option.



- We are satisfied
- We are not satisfied
- We are unsatisfied. We want better control and plan to move it back in-house
- We do not avail the service of an MSP

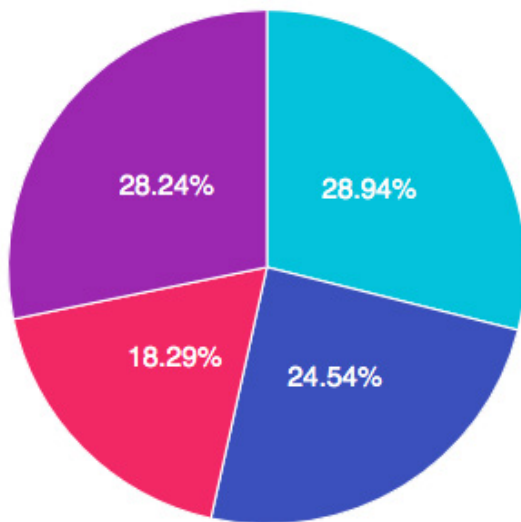
Q11

Are your users provided with self-service options, and are they effectively handling their own issues/requests?

The topline message here is that self-service failed to live up to expectations during the pandemic. When the 28.5% of organizations that still have no self-service capability – which are perhaps smaller organizations (that would benefit from self-service too) – are ignored, the survey shows

that only 40% of organizations found that [self-service](#) truly helped with IT support. For 35% of organizations, self-service helped less than expected. And for the final 25%, self-service adoption didn't take off.

Please note that this question also has a circa 80% response level, with it likely that the 20% that didn't respond had little to say on the topic. Either due to the absence of self-service within their organizations or a lack of success. Raising further concerns around self-service success.



- Yes, more than anticipated
- Yes, but less than anticipated
- No, self-service adoption did not quite take off
- We do not have self-service options for our users

For those that achieved it, self-service success played a significant role during the pandemic. For example, the “Yes, more than anticipated” option is correlated with both “We did a great job despite some hiccups” (from question 15) and “Yes, definitely” (from question 6). While the “We do not have self-service options for our users” option is correlated with “Unable to meet the challenge” (from question 15 again).

Additionally, organizations that are happy with their [MSP services](#) were far more successful with self-service than both those that were unhappy and those that didn't use MSPs.

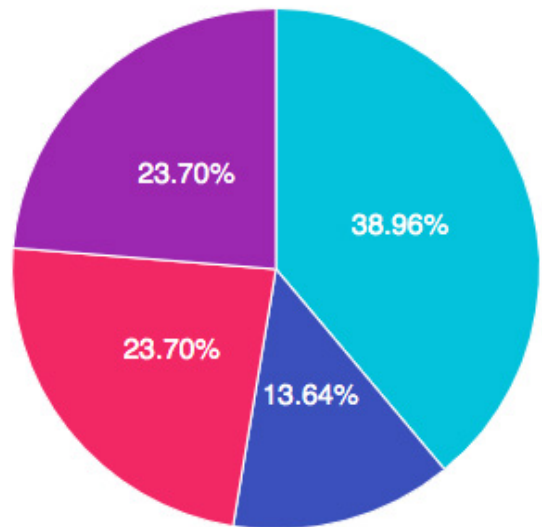
Q12

Do you think chatbots help with remote support?

Only circa 60% of survey takers answered this question. Plus, the way the question is phrased is forward-looking rather than related to what was achieved during the pandemic. So, please view the results in this context.

Ignoring the “We don’t use” responses, the majority of survey takers view [chatbots](#) as being beneficial for remote support at 50%. The minority (18%) don’t think that chatbots will help, with the final 32% unsure.

Interestingly, those organizations that use MSP services are far more likely to have voted “Yes” to this question. Perhaps a sign that MSP customers are either better informed on the potential of chatbots or early adopters.

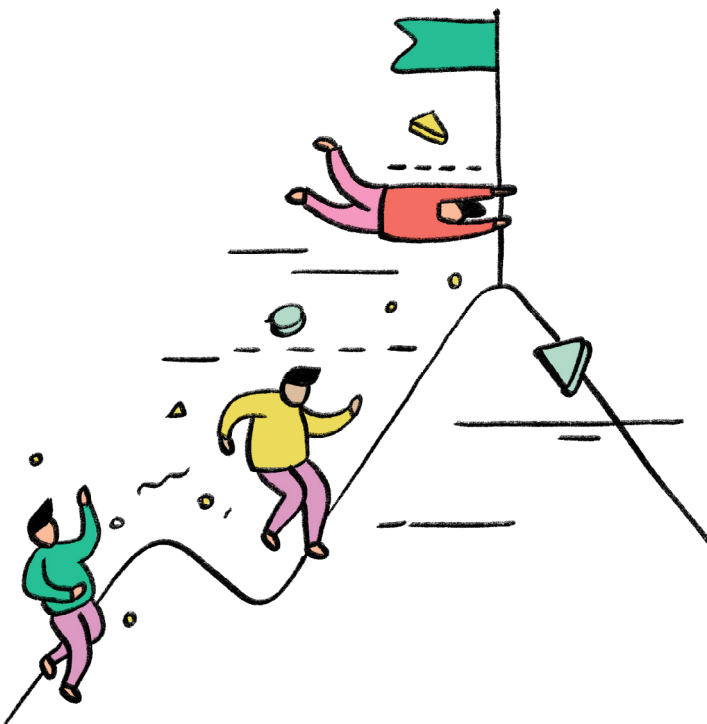


- Yes
- No
- I don't know. It's too soon to tell
- We don't use/have any chatbots in our ITSM tool

Business continuity success levels

The COVID-19 crisis severely tested the business continuity and disaster recovery capabilities of organizations – from the adequacy of plans to the real-world ability to implement them in a timely and successful manner. For many though, the pandemic’s impact will have been outside of planned-for scenarios due to the nature of its impact – preventing office-based working in many instances for IT service management personnel as well as the employees or customers they support.

Please also note that the following three questions all had a circa 80% completion level.



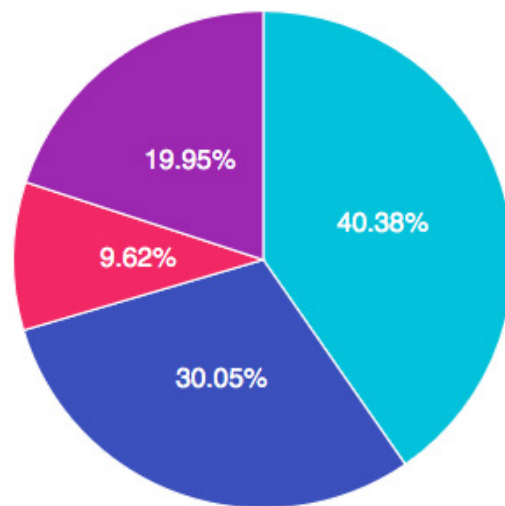
Q13

Did your business continuity plan (BCP) and disaster recovery plan (DRP) help you in this pandemic?

Worryingly, 20% of organizations had no BCP or DRP in place to help with the handling of the crisis and the emergency actions required to maintain both business and IT operations. Given that another 20% of respondents didn't answer this question, the lack of suitable plans could be even higher.

Of those that did have plans in place, the results were viewed as good – with half of respondents stating that they had good plans. And another 38% helped by their plans to some extent. Leaving only 12% of organizations for whom their plans were of little help.

Unsurprisingly, “We did not have BCP or DRP in place” is correlated with “Unable to meet the challenge” (from question 15). While “Yes, we had good plans to fall back on” is correlated with “We did a great job despite some hiccups.” And those organizations that are satisfied with their MSP services are far more likely to have had “good plans to fall back on” – probably because they, at least in part, benefitted from the MSPs’ plans. However, and oddly, the “Yes, we had good plans to fall back on” option does not appear to influence the future reputation of IT (as per question 6).

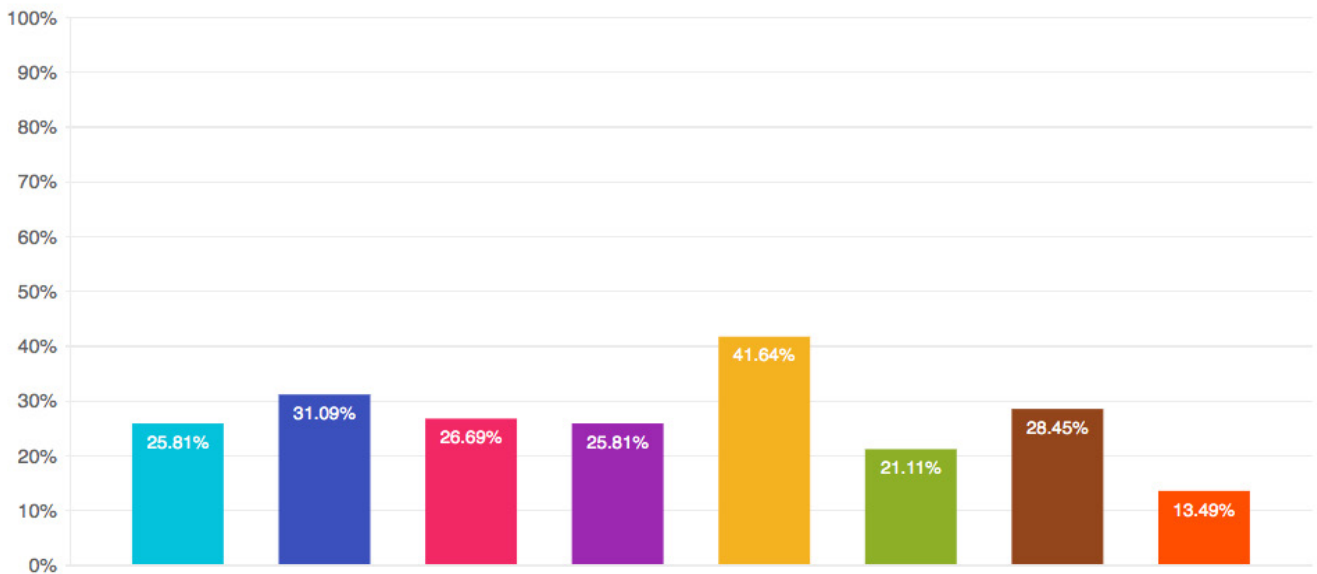


- Yes, we had a good plans to fall back on
- Not completely, but they helped some
- No, our BCP and DRP did not help us
- We did not have BCP or DRP in places

Q14

What areas were lacking in your BCP/DRP?

While not the most chosen option, worryingly, 29% of organizations with a plan stated that it had not been tested sufficiently prior to the pandemic. Outside of this, the responses were similar to the key challenges reported in question 2; other than security faring better in BCP and DRP terms.

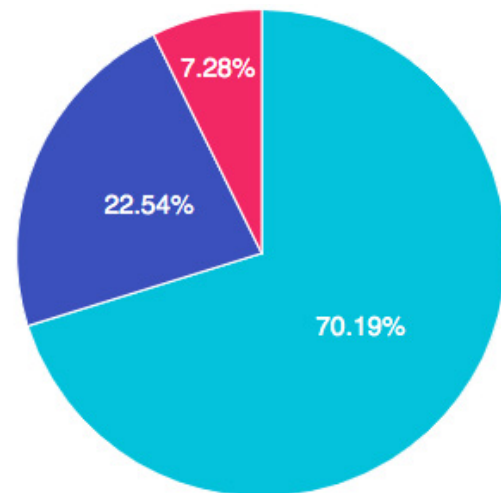


- VPN infrastructure
- IT asset and BYOD policies
- Team communication tools
- Security vulnerabilities
- Knowledge base articles and better documentation for end users
- Cloud workspaces
- Not enough prior testing
- Other (Please specify)

Q15

Overall, are you satisfied with the way the IT service desk team stood up to the challenges of remote work resulting from the COVID-19 pandemic?

The final question of the survey found that, despite all of the issues the pandemic highlighted, 70% of respondents felt that their IT service desk did a great job. With another 22% reporting that the service desk did an average job with much that could have been done better. Importantly, only 7% of respondents felt that the service desk wasn't up to meeting the remote [IT support challenges](#) that the pandemic presented.



- Yes, we did a great job despite some hiccups
- We did an average job, as there was a lot that could have been done better
- No, we were not able to meet this challenge

Survey summary and next steps

Question 15 is indicative of how the survey respondents feel about the IT support provided during the pandemic. That despite the difficult conditions [IT service desks](#), in particular, worked hard to keep employees, and the organization as a whole, working.

There is much to be learned from the COVID-19 crisis. In particular, related to IT support being more difficult than it needed to be due to a combination of inactivity, poor decisions, and a lack of spending across areas that include:

- **BYOD policies**
- **The provision of mobile-capable assets**
- **Cloud service adoption**
- **Self-service investments**
- **Business continuity planning.**

About ServiceDesk Plus

ManageEngine ServiceDesk Plus is ITIL-ready help desk software with integrated asset and project management capabilities. With advanced ITSM functionality and easy-to-use capabilities, ServiceDesk Plus helps IT support teams deliver world-class service to end users with reduced costs and complexity. It comes in three editions and is available in 37 different languages. More than 100,000 organizations across 185 countries trust ServiceDesk Plus to optimize IT service desk performance and achieve high end-user satisfaction. To learn more about ServiceDesk Plus and its features, please visit www.manageengine.com/service-desk.

About ManageEngine

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises — including 9 of every 10 Fortune 100 organizations — rely on our [real-time IT management tools](#) to ensure optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. We have offices worldwide, including the United States, the Netherlands, India, Singapore, Japan, China and Australia as well as a network of 200+ global partners to help organizations tightly align their businesses and IT.

For more information,

Website : www.manageengine.com

Blog: blogs.manageengine.com

LinkedIn: www.linkedin.com/company/manageengine

Facebook: www.facebook.com/ManageEngine

Twitter: [@ManageEngine](https://twitter.com/ManageEngine)

