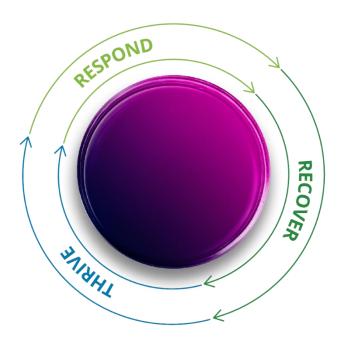# Deloitte.

The Q&A roundup series 2: Ensuring certainty in uncertain times – the evolving role of Command Centres
You asked, we answered.

Here are our responses to the questions you had in store for us, during our webinar on 'Ensuring certainty in uncertain times – the evolving role of Command Centres.'

How does work from home (WFH) impact the load on remote servers, including cloud infrastructure? How do we manage that?

The load certainly increases on remote servers and cloud infrastructure. Having said that, most IT Teams would have invested in platforms with easily scalable architectures and have in place, related vendor agreements to implement such scaling. All cloud platforms as you know, have built-in scale up and scale down options, which most IT Teams across companies, would have opted for, in terms of investment.

This rationale is derived based on the work we have done for clients, helping them formulate and implement their technology strategy and architecture, including cloud, and what we have seen happening in our client base.

How do we put together, in the fastest way possible, an effective real-time dashboard for the Crisis Command Centre (CCC)?

As indicated above, based on the work we have undertaken for clients in helping them choose the right business intelligence (BI) tools to implement dashboards, and what we have seen clients do, here are a few ways to enable quick dashboard implementation:

1. Quickly identify the business imperative: decide what KPIs the business and command centre want to view, and what drill-downs they need. Excel-sheet features can help make dashboard mock-ups faster.
2. Reuse existing artefacts to save time and focus on speed over elegance: leverage existing BI or BI deployments in your company, including the existing input data sources, to have dashboards up and running, covering most key aspects.
3. Tweaks and workarounds: quick tweaks can be made using self-service BI features in BI tools to make changes to existing dashboards relevant to COVID-19 responses. You can also use smart workarounds to on-board new data sources.

With respect to catering to our talent pool, what should be the north star in terms of concerns that should be managed/mitigated by the Command Centre from the onset?

At the onset of a crisis like this, the immediate concern for an organisation is always the safety of their employees and managing their whereabouts. We have seen clients using technology interventions to identify the whereabouts to manage repatriations and then use constant monitoring methods on people's health.

In parallel, organisations are also being empathetic to the fear psychosis that employees have and the most effective way to alleviate the fear of retribution and job security is by setting a conducive tone at the top, and communicating relentlessly and transparently over the course of the crisis.

Scenario planning is proving to be extremely difficult in this dynamic situation. What are some general guidelines to plan for various scenarios that could play out?

That's right, scenario planning is most effective when there is certainty around the various scenarios. However, in this crisis, possible situations are changing quickly. Hence, it is important to revisit your scenarios at a pre-defined frequency (for example, every fortnight) and accordingly plan the various aspects around supply chain, working capital, customer, etc.

How is a CCC different from a traditional command centre (Security operations centre (SOC), Network Operations Center (NOC), etc.)?

Traditional command centres are built specifically to serve a single purpose focussed on an operational outcome. For instance, a NOC monitors network traffic and flags-off link outage, traffic surge, etc. A CCC on the other hand enables an organisation affected by a crisis, to amalgamate all its resources and steer the crisis response and recovery efforts. The CCC acts as the nerve centre, orchestrating crisis response and monitoring the effectiveness of recovery efforts through close KPI monitoring. Organisational leaders are provided with rich actionable intelligence aiding swift, structured and effective crisis decision-making and constant communication with internal and external stakeholders.

What role will a CCC play in the future, considering the lessons learnt from the COVID-19 pandemic?

The CCC is expected to assume a centralised role and is likely to become a key differentiator in determining the resilience of an organisation. The ability to effectively respond to a crisis can be expected to determine the long-term viability of an organisation, while having an integrated, technology-enabled and secure CCC will provide positive assurance. In essence, the CCC can be expected to evolve from its current state and transform into a central engine which provides rich, proactive and actionable intelligence, in real-time, through a consolidated view of enterprise risks, robust crisis response and communication capabilities.

Where should the CCC be set up?

Organisations need to evaluate which location would suit them best, based on their specific needs and the infrastructure needed to support it. It could be from a designated individual's residence, any alternative location or a permanent alternative site. Resources and equipment could be distributed in a manner that allows seamless technological integration, to form a virtual set up. Moreover, communication protocols need to be clearly defined with a workflow. This entails listing out detailed communication steps or methods, channels to be used, etc. after these have been commissioned.

What kind of skillsets would you need to formulate an efficient CCC?

The skillsets required to man the CCC would vary, depending on the type of industry the organisation operates in and its nature of work. Based on the criticality of certain

functions, adequate representation within this taskforce would be necessary to provide information, situational awareness and feedback. These should be cemented by a single coordinator, empowered to make and take decisions. Typically a CCC may include an administrator, forensic experts, healthcare professionals, selected first-responders, financial analysts and a representative of human resources.

What are the information security considerations one should keep in mind while designing a CCC?

The personnel manning the CCC are expected to be privy to high levels of sensitive information. In addition to technological measures, including access control, system hardening and network segregation, emphasis on acceptable usage of information assets and information security awareness training is of paramount importance. Effective segregation of duties, coupled with periodic access rights and log-in reviews are necessary to ensure sensitive information is not being misused. The CCC should be designed using the 'secure by design principle' and 'defense-in-depth' principle.

In an order of priority, if we have to rate which supply chain functions or business operations take precedence (especially with limited cash flow availability), which would they be?

While specifying that each organisation will have their own unique challenges (for example, hospitality versus manufacturing; continuous process versus others, essential services versus non-essential services), in general, here is the order of priority that we see organisations across sectors follow:

1. Compliance to statutory obligations especially labour wages, followed by others, in the order of risk and impact of penalties levied. They secure their position through legal consultations and completion of formalities.
2. Minimising the cost of operations and prioritising spends based on organisational priority in terms of products/demands, plants/operations, and suppliers. They address issues related to inventory management (especially with regard to perishable items).
3. Ensuring business continuity and scalability when the situation improves, including;
   a) Workplace safety for employees/staff
   b) Prioritisation of key products, operations and suppliers
   c) Managing critical supply and closely monitoring for possible default. They also farm for alternate sources to ensure continuity.
   d) Responding to defaults in contractual obligations and exploring options of continuity or claims.
4. Compliance to other regulatory obligations and remediation plans such as anti-bribery and corruption, due-diligence, etc.

You mentioned an increase in contractual violations. Do you foresee all these violations leading to an increase in litigation and disputes? How do we gear up for this?

This situation is unprecedented and has impacted organisations across the world. Here are two scenarios we can envision:

a) Scenario 1: Vendors, as well as customers, may come forth with genuine situations relating to the crisis, and therefore fail to meet contractual obligations.

b) Scenario 2: A few vendors or customers may have defaulted on contractual obligations due to their own internal challenges even without the impact of COVID-19 and may attribute the default to COVID-19.

In the case of Scenario 1, we anticipate that the organisations may negotiate, to arrive at a mutually agreeable decision and look to support each other to maintain business continuity. The extent of flexibility may vary, depending on the strength of the relationship, criticality of the partner/client and impact on business continuity, current situation of financials of the organisation and the available buffer.

In case of Scenario 2, we anticipate more litigation to arise, especially with contracts that are critical for business continuity, or have higher penalty/claims associated with them.

In any of the above scenarios, organisations that are better prepared are likely to be able to maximise the benefits from such negotiations or litigations. Here are some areas that organisation should build their capabilities in:

• Ability to quickly gather information – contracts, transactions and KPI metrics including relevant documents in a digital format to monitor and identify (or anticipate) possible contractual violations, at the earliest.

• Ability to build scenarios and financial and legal models to arrive at decisions on litigation or negotiations and also decide the base and ceiling for negotiations

• Ability to arrive at templates of contract redressals based on scenario models

• Ability to document factual positions to enable negotiation or litigation support