Operational Resilience – Emerging Insights from 100 days of COVID-19 lockdown

By Prashant Shah, Executive Principal, AXCELERUS, LLC

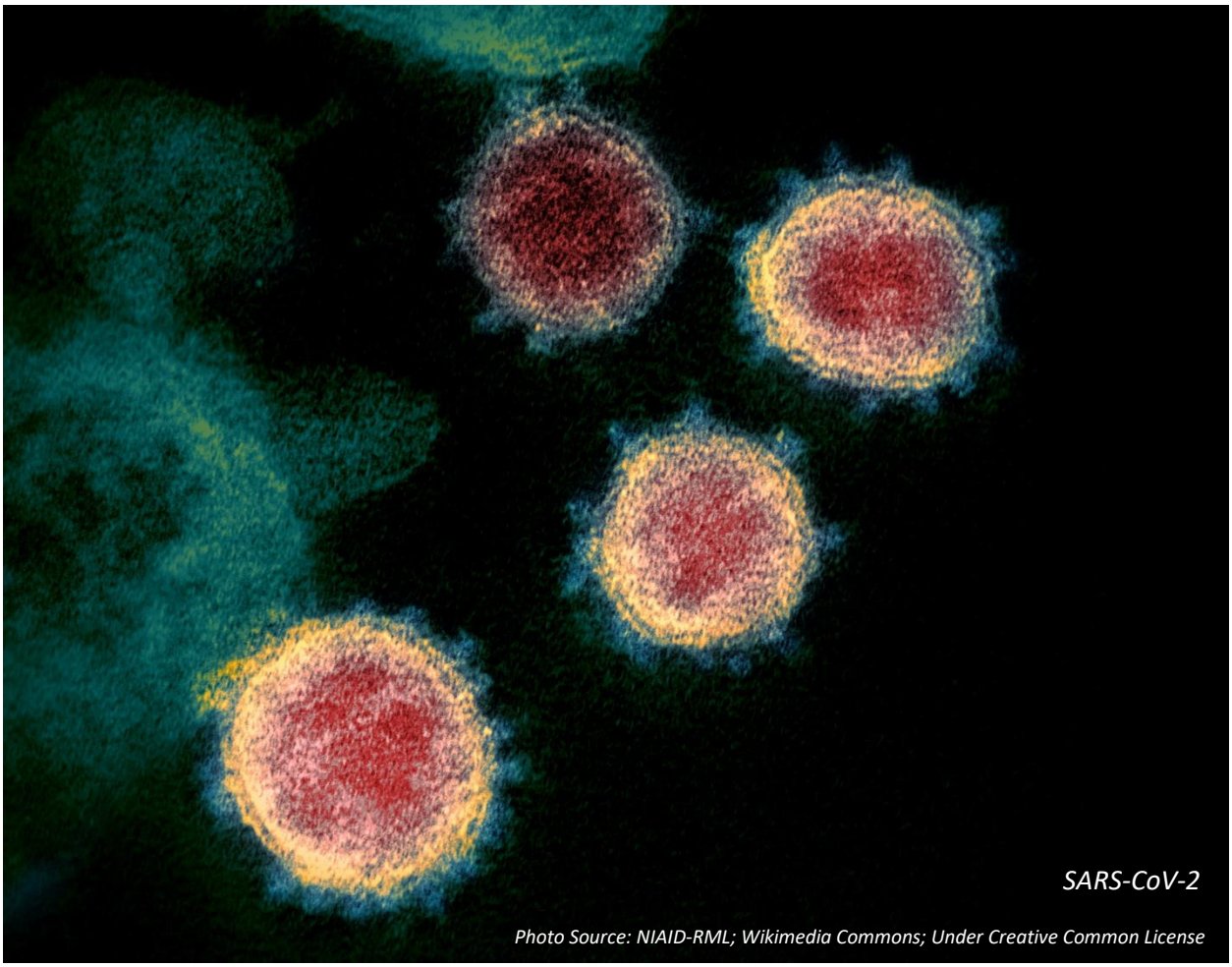


Photo Source: NIAID-RML; Wikimedia Commons; Under Creative Common License

Introduction

COVID-19 for most businesses felt like a Black Swan event. Even their Business Continuity Plans (BCPs) were impacted as practically most did not address the nature of lockdown or stay-at-home policies that were enforced globally. Whether business scrambled or had a relatively smooth sailing, we were keen to see if the 100+ days of lockdown due to COVID-19 highlighted an area of operational risk that were either new or an existing risk area that took on a significant proportion. So, we asked our clients, vendor partners, and consulting partners one question:

"In the past 3 months, as you transitioned to work from home, what was one key operational risk that was amplified or newly discovered?"

And what we found was a story of Operational Resilience. Collectively a number of operational risks came up as areas where they struggled, but most were able to manage the transition.

We summarize the findings from the 30+ responses we obtained under 5 key Operational Risk areas in the hope that you use this opportunity to further increase your Operational Resilience.

Operational Risk Area 1: Technology and access

With work from home becoming mandatory, companies without cloud based turrets were compelled to invest in one when installation of physical turrets become nearly impossible. This transition also put pressures on the Confirms group, and cases where things fell through the cracks were also observed.

Photo Source: Foreign Economic Espionage in Cyberspace; Wikimedia Commons; Under Public Domain

Bandwidth was another area where companies with scalable VPN infrastructure experienced limited disruptions. Network latency become important especially for front office trades as well as for real-time monitoring and trade surveillance. Network outages and the resultant lack of access to apps was an area where people complained of it being a major irritant. Loss of real-time communications at one company resulted in communications delays and a missed opportunity in managing ships and other logistics. Risks in stability of IT and communications infrastructure were amplified and became a key point for company responses and investments.

Poor authenticated access control was another highlighted area of risk. One company responded with moving from one-factor authentication to two-factor authentication.

People also expressed concerns in the area of cybersecurity. Security of collaboration tools and virtual processes become important. Cyber hygiene and enforcement of company policies related to adhering to proper cyber protocol became apparent.

Operational Risk Area 2: Data security

Photo Source: Foreign Economic Espionage in Cyberspace, Wikimedia Commons; Under Public Domain

Another interesting area of risk that became apparent was the exposure of internal data layers (i.e. internal SharePoint data) to external locations via remote desktop or host interaction as well as through non-secure file sharing -- all coupled with poor authenticated access control.

Inadvertently sharing one's client or confidential information with another party while sharing screens was also identified as a key data security risk.

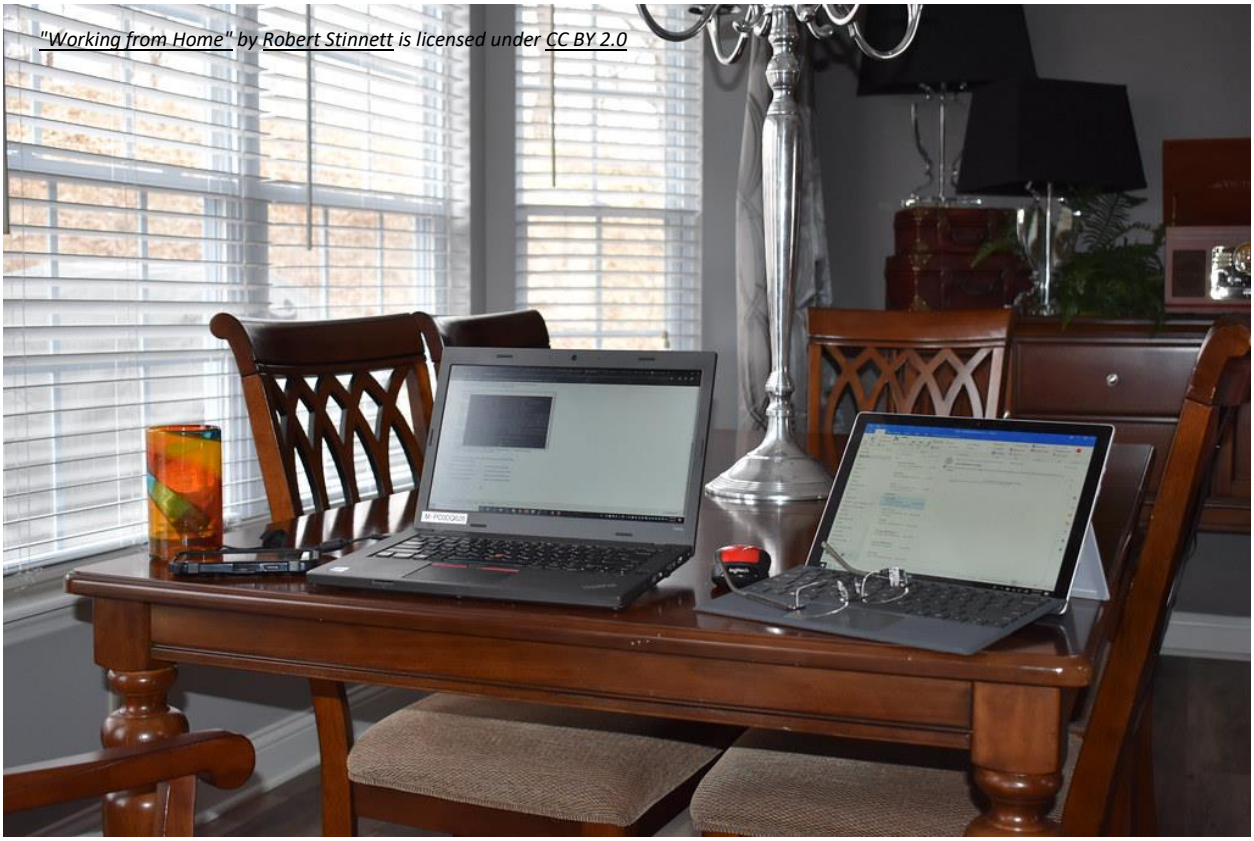
One respondent highlighted challenges in maintaining physical data security for documents and processes that are difficult to digitize.

The lockdown also highlighted siloed data repositories and analytics platforms as well as risks from non-digitized processes and spreadsheets and non-synchronized updates.

We believe data security is an area companies need to continue to monitor and invest. While VPN may provide a line of defense, companies need robust policies and enforcement to ensure data security protocols are followed and become part of remote access culture.

Operational Risk Area 3: Communications

While many people complained of an overload of virtual meetings, some missed the spontaneity and effective collaboration of a team sitting in one room and potential quicker resolution of issues. Risks of missing non-verbal cues and teams heading in different directions were also highlighted. Others found the benefit of teams adhering to meeting protocols and self-solving issues to reduce the need to meet.



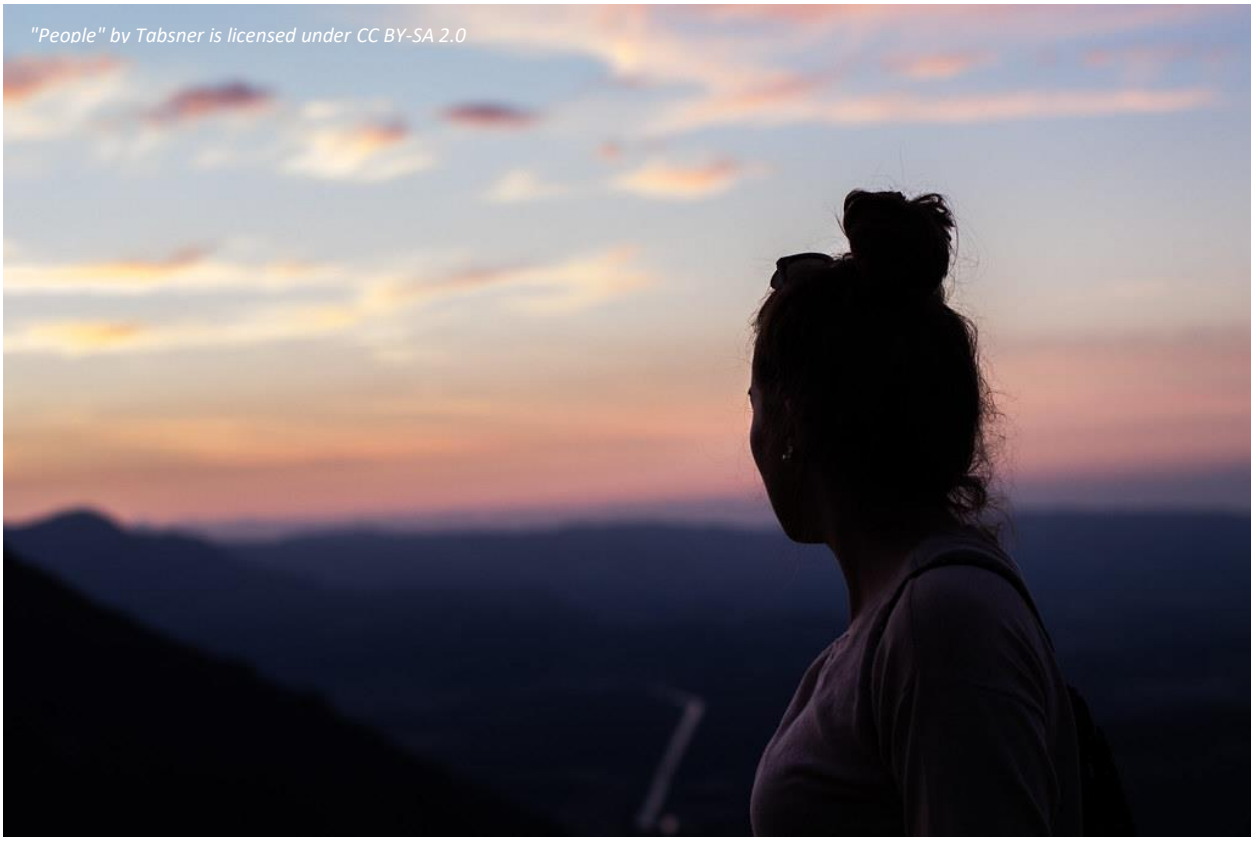
One company found certain communications channels did not work as expected and had to scramble to find alternate mechanisms.

A respondent highlighted the challenges in maintaining confidential communications from home where multiple people worked from home and there were space constraints.

A concern about people being improperly dressed for meetings with external parties was also highlighted.

Operational Risk Area 4: People

A number of risks well highlighted related to well-being people and impact of extended working from home. Potential mental health issues from the monotonous nature of work to staff burnout due to both isolation and longer hours as well as impact due to lack of vacation time and anxiety were highlighted.



Many folks liked working from home and saving both travel and grooming time. This newfound time has resulted in an increase in productivity.

Non-availability of child-care support and working from home has highlighted challenges for some families as they tried to cope up with both responsibilities. These responsibilities have had an impact on productivity which some believe were camouflaged by employees working longer.

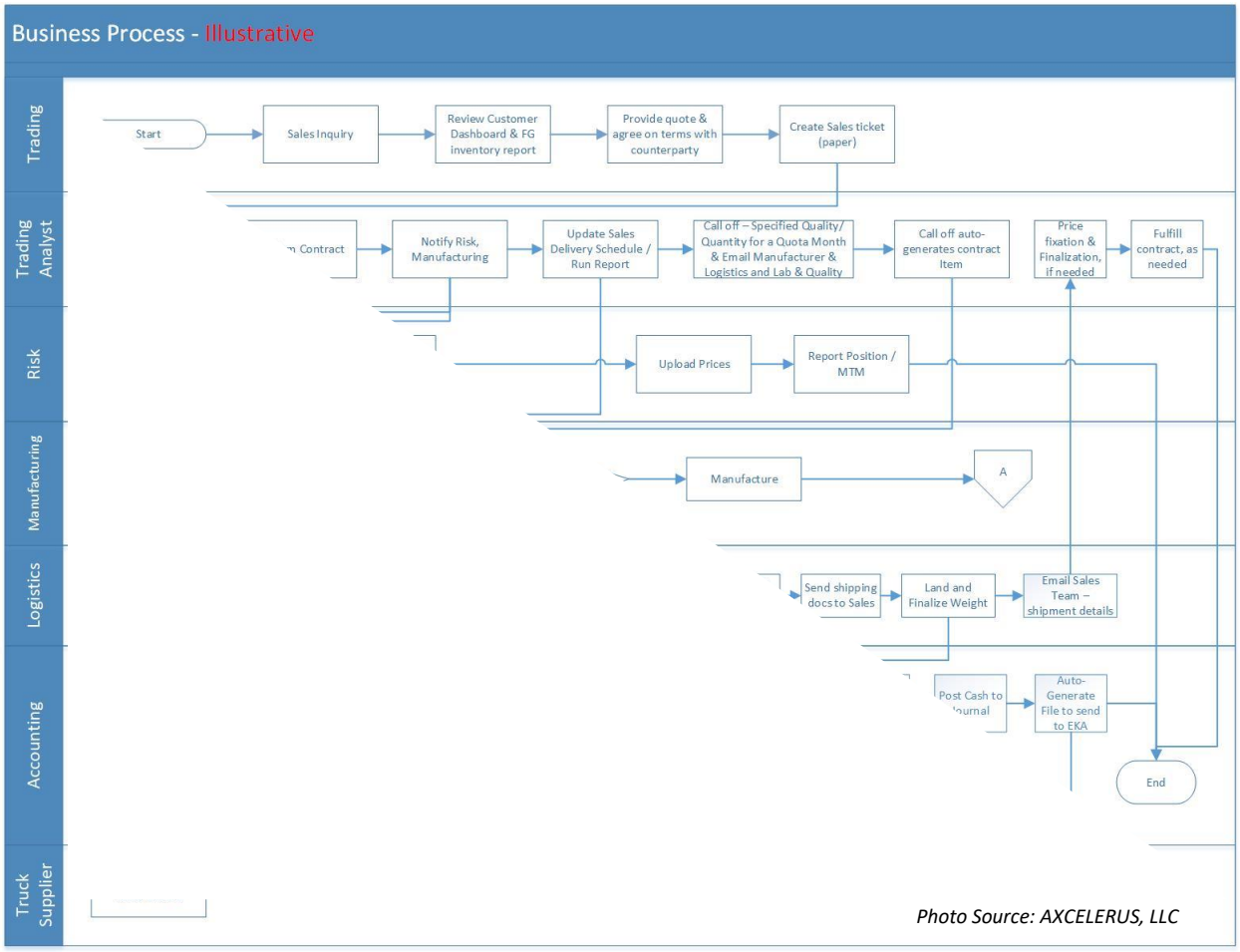
Another interesting finding was the loss of balance within the team; inefficiencies of non-performers coupled with increased performance among others seemed to hold the team back and thereby increased load on managers overseeing work.

Interestingly, one respondent indicated that COVID-19 highlighted the importance of having good leadership at the top.

Operational Risk Area 5: Processes

Work from home highlighted redundancy in work (and personnel) as more processes were forced to digitize.

T+1 compliance processes generally worked as expected but supply chain processes were impacted and created challenges.



External interfacing process (e.g. customer or investor facing processes) were impacted the most as COVID-19 put restrictions on travel, which resulted in deals getting consummated. Business development processes reflected increased lead time and more follow-ups.

Acceptance of digital signatures and need for document management systems and streamlining of contracting processes was another area that required attention.

As more companies moved to cloud based processes, the weak links in the form of manual processes and local spreadsheets came to the fore and impacted the migration to cloud.

We believe companies will need to monitor the process that are difficult to digitize (for example, inspection processes in supply chain or logistics) and potentially invest in industry wide efforts to develop digital and contractual protocols to manage the same.

Smoother Transitions

Companies with high degree of virtualization and remote work policies were able to manage the transitions better. In fact, many respondents indicated that they did not miss a beat while working from home as the team was used to doing so. They also reported no significant increase in any operational risks they were tracking.

In conclusion

While companies had smoother or initial rough transitions, they displayed Operational Resilience in managing the transition. While companies are working to adjust to the "new normal," we believe data security, mental health issues, and external facing processes are areas where companies need to watch unexpected escalations. Being proactive in these areas will further enhance their Operational Resilience.

About the Author

Prashant Shah is Co-Founder and Executive Principal at AXCELERUS, a specialized E/CTRM consulting practice with global client-base and solutions for the full spectrum energy and commodity transacting value chain. Prashant focuses on risk management activities, risk reporting, front, middle and back-office processes and energy transacting/risk management (ETRM) systems, including project management and implementations.
Prashant can be reached at prashant.shah@axcelerus.com.