June 18, 2020

The Case for the COVID-19 Risk Register

by Anthony D. Glosson

Please note: The below information may require updating, including additional clarification, as the COVID-19 pandemic continues to develop. Please monitor our main COVID-19 Resource Center and/or your email for updates.

The current COVID-19 pandemic has upended supply chains, shifted entire sectors to remote work business models, and necessitated improvisation on a daily basis, all with little to no lead time. As we assist clients in navigating a rapidly-changing world, we are always conscious of the fact that the business continuity and cybersecurity threat landscape is evolving alongside it. While sound risk management strategies will look different for each organization confronting these challenges, one tool is indispensable: the risk register.

Popularized by the U.K. government and used by businesses the world over, the risk register is tailor-made for managing massive disruptions like those precipitated by COVID-19. To date, the risk register has seen greater adoption among businesses based abroad than those here in the United States, but with the current pandemic, the time has come for everyone to become comfortable with this tool.

COVID-19 risk registers are quick to stand up, easy to scale, and we consider them to be an indispensable weapon in a business' risk management arsenal.

What is a COVID-19 Risk Register?

Risk registers are simple tools by design. They can be housed in a word processing document, a spreadsheet, or through more sophisticated technologies. In each case, the core elements are as follows:

1. Document significant operational changes due to COVID-19
2. Identify risks created by these changes
3. Designate mitigation measures
4. Track implementation of mitigation measures

National security-oriented readers will recognize that these components closely track the OODA loop, the military action cycle consisting of Observe, Orient, Decide, Act. Successful organizations control their own fate by staying ahead of this curve.

As in warfare, COVID-19 business decisions are made against the backdrop of quickly-changing circumstances

on the ground, and the COVID-19 risk register offers an essential framework for informing those choices. The risk register accomplishes this by keeping the spotlight on operational changes and then offering a structured method to identify and mitigate the derivative risks.

Crucially, a risk register is crowdsourced. Decision-makers at every level in a business should be empowered to submit descriptions of operating changes for inclusion in the risk register and, to the extent they are able, contribute to the other three components of the risk register as well. Businesses can accomplish this by maintaining group-editable spreadsheets, adding a link on internal portals, setting up dedicated email mailboxes, or through any number of other means.

Businesses then assign a keeper for the risk register. The keeper may be an individual or a working group, but in all cases, the keeper should have sufficient insight into the business' cybersecurity and business continuity initiatives to recognize the risks posed by any identified operating changes. The keeper completes items 2-4 on the risk register or, if already completed by the business component that submitted the operational change, the keeper verifies the adequacy and propriety of what has been submitted. The keeper also adds any other items to the risk register that may be appropriate given the nature of the business and its existing risk management strategies. Some additional items to consider for inclusion are:

- Severity of risks
- Duration of risks
- Internal policy compliance status
- Responsibility for particular risks and mitigation tasks

Here is an example of what a simple COVID-19 risk register may look like:

Operating Change	Derivative Risk(s)	Risk Severity	Risk Duration	Policy Reference	Mitigation Measure(s)	Mitigation Status	Point of Contact
Increased volume of online sales and limited call center availability has required reducing automated credit card purchase authentication measures	Heightened exposure to fraudulent purchases	High	Temporary – until call center capacity can be scaled up	Payment Card Policy Section X.X	Index shipping addresses against past purchases	Implemented	Dana Scully (IT)
	Possible violation of card issuer agreements	Medium	Temporary – until all authentication measures are re-enabled	National Procurement Policy Section X.X	Review issuer agreements for terms	In process	Fox Mulder (Legal)

Why Implement a COVID-19 Risk Register?

Operational changes come with risks, particularly when undertaken on short notice. And if savvy risk management means understanding one's risk posture at any given time, then disruptions like COVID-19 turn that objective into a moving target.

A risk register confronts this challenge head-on by providing an avenue for real time documentation of operational changes. After the fact, it may be immensely resource-consuming or even flat out impossible to reconstruct each improvisation or deviation from standard operating procedure by memory or observation. Things inevitably slip through the cracks, and that leaves you with an incomplete understanding of your business' risk posture. Your colleagues' ingenuity and adaptability become blind risk vectors.

Maintaining a risk register allows you to get ahead of the OODA loop on these changes. As internationally-inclined readers already know, Article 30 of the EU General Data Protection Regulation requires organizations to maintain a data processing register for related purposes. Much like logging data processing activities, tracking operational changes with a view toward derivative risks gives an organization a holistic picture of its overall risk posture, enables the business to coordinate its risk management efforts across departments, and puts it in a position to make decisions informed by up-to-date facts on the ground rather than relying exclusively on the assumptions built into its policy documentation and preexisting playbooks.

This operational focus gives risk registers a distinct advantage over traditional risk assessment tools, which frequently begin with an identified risk and then analyze the potential implications of that risk. In times of massive disruption, the challenge is spotting and managing a litany of new risks, not merely getting a handle on a set of risks that have already been identified.

Moreover, maintaining a risk register helps to document the context for business decisions made in the proverbial fog of war, where the best information at the time of a decision may be outdated by start-of-business the following day. It demonstrates that an organization is risk-aware, thoughtful, and deliberate about its approach to an unprecedented situation.

In short, you should maintain a COVID-19 risk register if you want the ability to explain to customers and regulators why you are confident that you'll emerge stronger from this crisis.

How Can a COVID-19 Risk Register Help Reopen My Business?

As C-suite conversations turn from resiliency to reopening, a COVID-19 risk register can help answer the most pressing questions. Most significantly, maintaining a risk register helps to understand how your day-to-day business operations are different today than they were in the Before Times. Which activities is your business equipped to perform, over what time horizons, and at what scale? What previously-unremarkable events might generate significant exposure for continuity of business given an organization's new risk profile?

Further, many of the changes necessitated by COVID-19 may reveal heretofore hidden efficiencies or demonstrate that longstanding fears were unfounded. Maintaining a COVID-19 risk register equips a business to build a strategy for phasing out operational changes—or deciding to keep them—all centered around risk-savvy analysis of the likely long-term implications of those choices.

Finally, keeping a COVID-19 risk register brings internal policy compliance into focus. Decisions made in triage mode may leave an organization in violation of its policy documentation, even when the cybersecurity or business continuity impact of those decisions are relatively minor. Assessing compliance status in a regimented fashion puts a business in a position to reopen with confidence about its degree of policy compliance—and to reduce litigation and regulatory risk in the process. And in cases where applicable policies no longer reflect the new reality, the information collected in the COVID-19 risk register will assist with reshaping policies in a sustainable manner. Going forward, policy documentation with pre-2020 update timestamps will be inherently suspect, and the risk register is an invaluable tool for identifying exactly which policy updates 2020 should bring.

Okay, Give Me Some Examples

Still unpersuaded of the value added by maintaining a COVID-19 risk register? While every organization will have made different operational adjustments, consider whether you're aware of the responses to the following questions and what you might learn by assessing their combined effects and any mitigation measures as part of your overall risk posture:

- How has error reporting and support monitoring changed?
    - What new requests are coming in?
    - How do they compare to typical requests?
- Do data loss prevention (DLP) processes function externally?
    - Do they require VPN connections?
    - What other limitations exist?
- How does encryption function for files open in remote access? What are the new risks imposed by remote editing in collaborative environments?
- Where is sensitive data being stored on local systems?
    - Is there a change in the type/amount of data collected?
    - Is there a change in storage location or data flows?
- Is your network infrastructure capable of accommodating the shift in resource demand? E.g., bandwidth bottlenecks may necessitate routing non-essential users through third country VPNs.
- If hiring new employees, what changes have been made to onboarding process? Are you still provisioning email accounts from same provider? Has browser-based email access recently been enabled, and what compensating protections have been implemented in those cases?
- If furloughing employees, how are systems and data being temporarily secured in the interim?
- If employees are terminated, how is access to confidential information disabled—including any data stored locally on employees' devices?
- With new groups of employees working remotely, have you defined new flags to identify suspicious behavior from each user group? E.g., failed login attempts, unusual IP addresses or geolocations, extensive or erratic file downloads or deletions, etc. These may be different from the identified flags for preexisting remote work groups.
- How has two factor authentication been rolled out to new groups of remote work employees?
- How is compliance training and incident response readiness occurring for new and existing employees?

- How are invoices approved and settled? Any changes to the process that introduce vulnerabilities?
- Do newly-adopted communications technologies present new threat vectors?
- Have anti-theft mechanisms been moved to remote settings?
    - What inventory control mechanisms exist, and have they accounted for irregular demand and inconsistent supply chain flow?
    - How is register cash reconciled, particularly if circumstances have dictated till-sharing among employees?

Armed with the answers to these questions and others like them, your business can determine how best to coordinate resiliency with vendors, project responsibility and competence to customers, mitigate regulatory and enforcement risk, and even anticipate market trends in the critical months to come.

The Bottom Line

A COVID-19 risk register provides businesses with a centralized database of operational changes implemented in the process of addressing the current pandemic. By focusing on operational changes and then determining risk vectors from there, a COVID-19 risk register puts businesses in a position to navigate rapidly-changing circumstances in an organized strategic fashion. In so doing, the COVID-19 risk register helps mitigate regulatory, litigation, business continuity, and cybersecurity threats, while offering reassurance to customers, employees, and other stakeholders.

Further discussion of reasons for and uses of risk registers can be found here. If you need assistance standing up or refining your COVID-19 risk register, our COVID-19 team is closely attuned to the latest developments in business continuity, resiliency, and public health innovation in the face of the coronavirus crisis. Please reach out to your primary KTS point of contact or send us an email at #COVID-19KTSTaskForce@kilpatricktownsend.com.