Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Thwarting risk in your company's Supply Chain

An e-Book publication sponsored by Galvanize

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 6,300 customer organizations in 130 countries, Galvanize is connecting teams in many of the Fortune 1,000 and S&P 500 companies, and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

Visit wegalvanize.com to learn more. Follow us on Twitter, LinkedIn, or see what we're up to on Instagram.

Inside this e-Book

Blockchain: New frontier for managing supply chain risk

A pilot project being explored by the U.S. FDA has enlisted IBM, KPMG, Merck, and Walmart to tackle how to incorporate blockchain into pharmaceutical supply chains. **Jaclyn Jaeger** has more.

For all the times you've been to a grocery store, have you ever wondered which farms those fruits and vegetables originated? What about the last time you went to a pharmacy? Have you ever stopped to think about the quality and safety of those drugs, and how and where they were formulated?

Thanks to blockchain technologies, supply chain teams can now track the safety and traceability of products and data across the entire supply chain in ways—and at speeds—once unimaginable.

That is the impetus behind a new blockchain pilot project currently being explored by the U.S. Food and Drug Administration in the pharmaceutical industry, which is more broadly seeking how to incorporate blockchain into pharmaceutical supply chains. As part of this effort, the FDA in early June selected four organizations—IBM, KPMG, Merck, and Walmart—to take part in the pilot project.

Blockchain is open-source software provided through a digital ledger system, organized by a series of chronologically grouped transactions (blocks). These blocks are stored and secured on a peer-to-peer network using cryptography technology and managed by sophisticated mathematical algorithms.

In the context of the pharmaceutical industry, blockchain gives supply chain leaders the ability to track pharmaceuticals from the moment they are manufactured in the plants to the point of sale, directly to the customer. Further, blockchain is designed to establish a permanent record and may be integrated with existing supply chain and traceability systems.

In this context, the FDA through its proposed peer-to-peer network aims to:

» Help reduce the time needed to track and trace inventory;
» Allow timely retrieval of reliable distribution information;
» Increase accuracy of data shared among network members; and
» Help determine the integrity of products in the distribution chain, including whether products are kept at correct temperatures.

The push behind this complex undertaking began in November 2013 with the enactment of the Drug Supply Chain Security Act (DSCSA). Among other things, the DSCSA mandates the creation of an electronic, interoperable system to identify and trace certain prescription drugs as they move through the U.S. supply chain. This must be achieved by 2023.

"Blockchain's innate ability within a private, permissioned network to provide an 'immutable record' makes it a logical tool to deploy to help address DSCSA compliance requirements," Arun Ghosh, KPMG blockchain leader, said in a joint statement announcing the pilot project. "The ability to leverage existing cloud infrastructure is making enterprise blockchain increasingly affordable and adaptable, helping drug manufacturers, distributors, and dispensers meet their patient safety and supply chain integrity goals."Mark Treshock, IBM global solutions leader for blockchain in Healthcare & Life Sciences, also touted the benefits of blockchain, which "could provide an important new approach to further improving trust in the biopharmaceutical supply chain," he said.

"We believe this is an ideal use for the technology, because it can not only provide an audit trail that tracks drugs within the supply chain, it can track who has shared data and with whom without re-

vealing the data itself," Treshock added. "Blockchain has the potential to transform how pharmaceutical data is controlled, managed, shared, and acted upon throughout the lifetime history of a drug."

Other blockchain efforts

Each organization selected by the FDA—Walmart, Merck, IBM, and KPMG—brings to the pilot project extensive experience and technical knowledge in implementing blockchain technology for the enhancement, safety, and traceability of products. For example, prior to joining the FDA as deputy commissioner for food policy and response, Frank Yiannas was vice president for food safety at Walmart, where he was involved in a blockchain pilot that traced mangoes back to their source.

"I bought a package of mangoes at a local Walmart and asked my team to find out which farm they came from," Yiannas explained in remarks at the International Association for Food Protection on July 22. "Working with each stakeholder in the supply chain, they identified the farm in a mere six days, 18 hours, and 26 minutes—and that was pretty good when the average traceback can take weeks or even months."

"Fast forward to the pilot using blockchain technology to trace mangoes from farms in Mexico to two stores in North America," Yiannas continued. "For this test, each stakeholder in the supply chain—including farms, packing houses, transportation companies, importers/exporters, processing facilities, distribution centers, and stores—put data on the blockchain. The blockchain linked these blocks of data together to show the journey this mango took from farm to store."

Rather than take seven days to trace the mangoes, it took just 2.2 seconds. "That is what I have referred to as 'food traceability at the speed of thought,' " Yiannas said.

Following successful blockchain pilots like these that provide enhanced traceability in some of Walmart's food products, "we are looking forward to the same success and transparency in the biopharmaceutical supply chain," Karim Bennis, Walmart's vice president of strategic planning and implementation, health and wellness, said in the joint statement.

For its part, IBM, since first launching its blockchain-as-a-service in 2016, has worked with hundreds of clients, including in the healthcare space, to implement blockchain applications and will provide use of its cloud-based Blockchain Platform.

Group effort

The FDA's pilot project is just one of several initiatives exploring blockchain's application in the life sciences industry. Many of these initiatives are being led by blockchain technology providers.

One such example is the MediLedger Project, led by Chronicled, a blockchain technology firm. First established in 2017, the focus of the MediLedger Project was to evaluate the feasibility of a blockchain solution for compliance with the DSCSA. The resulting prototype was a joint effort among pharmaceutical companies Pfizer, Genentech, Amgen, and Gilead and pharmaceutical wholesalers McKesson, AmerisourceBergen, and Cardinal Health. These companies have since been joined by FFF Enterprises, Dermira, Eli Lilly, Walgreens, and Walmart.

On June 18, the MediLedger Project announced the start of its participation in the FDA's pilot project. The MediLedger Project said the aim of its pilot will be to explore and evaluate methods to enhance the safety and security of the drug supply chain by utilizing its earlier built blockchain-based solution.

"Years ago, we saw an opportunity to build a more efficient system and, together with industry partners and peers, we are strategizing to develop solutions that build in greater efficiencies, effectiveness, and safety into the supply chain," said Scott Mooney, VP of distribution operations at McKesson. "This is just the beginning of the type of industry-altering impact new technologies like blockchain will have."

The FDA's pilot project is scheduled to be completed by 2019 year-end, and the results are expected to be published in an FDA DSCSA program report. At that time, the project's participants will evaluate next steps. ■

Poll: gaps in integrated risk management

Many organizations' ERM capabilities aren't as integrated as they need to be, leaving them vulnerable to legal, financial, regulatory, and reputational risks, says a recent survey. **Jaclyn Jaeger** explores.

Compliance and risk professionals know that having an enterprise-wide view of risks is far more effective than trying to manage risks in a fragmented way, and that achieving this objective through automation is far more efficient and cost-effective than manual processes and controls. Even knowing that, however, many organizations' enterprise risk management (ERM) capabilities still aren't as integrated as they need to be, leaving them vulnerable to legal, financial, regulatory, and reputational risks.

That was just one of many key findings to come from a recent governance, risk, and compliance (GRC) benchmark report conducted by Compliance Week, in partnership with Riskonnect, an integrated risk management solutions provider. The survey polled 113 compliance, risk, and audit executives from around the world—including the United States, Europe, Asia-Pacific, and Latin America—to get a better sense of the state of organizations' risk management capabilities; how effective they are at mapping risks; what GRC metrics they track; and much more.

According to the findings, 44 percent said they have "standardized some processes and use of

technology but not across the entire enterprise," while another 35 percent said their processes and technologies remain largely siloed. Only 20 percent said they have integrated processes and technology across the organization.

Most respondents (62 percent) further indicated they are only "somewhat confident" in their organization's ability to map each control it has to a given risk or requirement. Another 21 percent of respondents said they are "very confident," while 14 percent said they are "not confident."

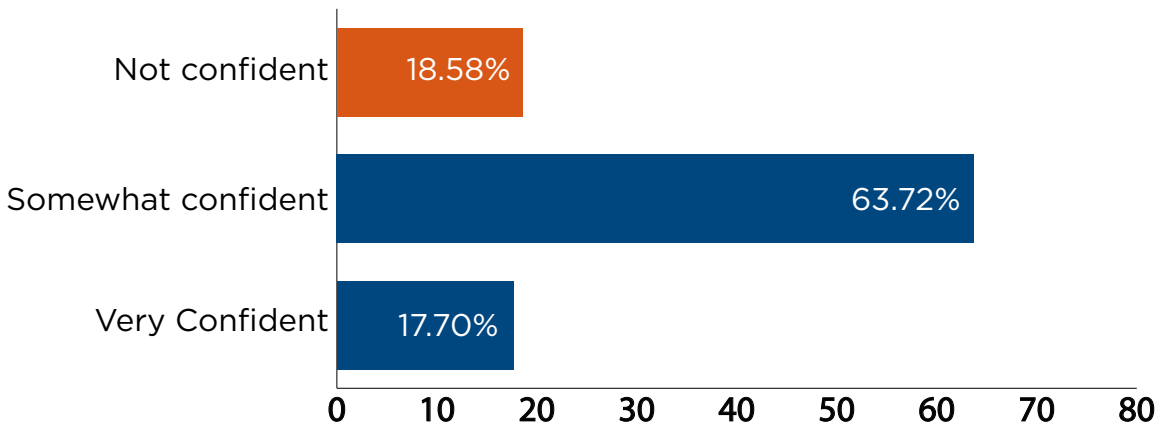
"In my experience, most organizations rely on localized and manual solutions for all kinds of risk management needs," says Quin Rodriguez, vice president of strategy and innovation at Riskonnect. "This amounts to complex, confusing tangled webs of IT systems and data sources that can't support effective enterprise risk management."

"If integrated risk management is the corporate goal, a key strategy to get risk management working effectively and efficiently throughout the enterprise is to adopt a unified framework and create a common risk vernacular," Rodriguez says. The follow-up question, then, is how to go about integrating those processes and technologies, he says.

That is where an integrated risk management solution, like the one offered by Riskonnect, comes into play. Riskonnect's integrated risk management solution consolidates in a centralized dashboard information from multiple sources, automates routine processes, and uses sophisticated analytics to turn complex data into actionable intelligence. In this way, the comprehensive, web-based system supports risk, compliance, and internal audit, delivering deep visibility to better manage things like vendor risk management, health and safety, policy management, and claims administration.

An integrated risk management solution also helps compliance and risk functions track key metrics. According to the survey, the top five key performance indicators respondents said they track are the number of substantiated allegations of miscon-

How confident are you in your organization's ability to map risks to the drivers of each risk across all functions?



Sources: Compliance Week; Riskonnect

duct; risk coverage; number of control violations; number of control-test failures; and total cost of risk, compliance, and control activities.

Risk ownership

Risk managers and risk owners are another important part of a best-in-class risk management program. When asked who leads strategy around integrating GRC processes, 30 percent answered the chief compliance officer, while 21 percent said the chief risk officer, and 16 percent said they had no such role. Fewer said it was the chief executive officer (15 percent) or chief audit officer (8 percent). Here, it all depends on "who has the most visibility across the organization with access to leadership," Rodriguez says.

What is imperative to a robust ERM program, however, is having the ability to map ownership of each risk, requirement, and control to a specific individual or role. This helps ensure proper oversight of a specific operation.

When asked how confident they are in their organization's ability "to map ownership of each risk, requirement, and control to a specific individual or role," however, 61 percent said they are only somewhat confident, while another 15 percent said they are not confident at all. This is concerning, because "if you don't designate an owner of a risk, then how do you manage it?" Rodriguez says. "Who do you hold accountable?"

Furthermore, most respondents (64 percent) expressed just mediocre confidence in their organization's ability to map risks to the risk drivers across functions, while 19 percent said they are "not confident." Just 17 percent said they were "very confident." To ensure that risk drivers are properly mapped to each function, many organizations today delegate responsibility for risk-information gathering to several risk owners across the various business functions, with the process overseen by a central risk team.

Not surprisingly, many respondents indicated they have the least amount of confidence in their organizations' ability to identify vendor and other third-party risks, with 27 percent saying they are "not confident" in their ability to do so. The types of third-party risks organizations should watch out for include reputational/social media risk; financial; cyber; operational; and supply-chain.

"Having the ability to integrate more points of the business allows organizations to really automate the risk controls process. It allows people to see the risk landscape far better than they ever had before and understand the impact it has on their organization."

Quin Rodriguez, VP of Strategy and Innovation, Riskonnect

Effective third-party risk management (TPRM) helps companies identify high-risk behaviors and situations, monitor vendor risk levels over time, and compare the risk levels of vendors against one another. When TPRM is integrated with sophisticated technology and the risk posture of the organization, it provides even greater visibility, risk reduction, and cost savings. In a 2018 Compliance Week on-demand Webcast, Riskonnect further discusses how an integrated approach helps solve TPRM challenges.

"Having the ability to integrate more points of the business allows organizations to really automate the risk controls process," Rodriguez says. "It allows people to see the risk landscape far better than they ever had before and understand the impact it has on their organization." ■

Top 10 supply chain risks of 2019

Natural disasters, droughts, cargo theft, and industrial fires are some of the top supply-chain risks from 2019, writes **Jaclyn Jaeger.**

A recent report, based on risk and incident data collected by DHL's cloud-based risk management provider Resilience360, presents a global overview of major events that disrupted supply chains in 2018 across five key regions: North America, Europe, Latin America and the Caribbean, Africa and the Middle East, and Asia Pacific. It further provides a list of the top 10 supply chain risks to watch in 2019:

1. Global trade wars and Brexit. Global trade wars between the United States and the rest of the world will continue to impact many manufacturing supply chains, due to the imposition of U.S. tariffs and the consequential retaliatory tariffs that many countries have placed on a wide range of consumer products and components, impacting nearly all industries.

Some companies, however, are turning this risk into opportunity. For example, U.S. motorcycle maker Harley Davidson announced last year that it would shift production of its motorcycles for EU destinations out of the United States to Thailand to avoid EU tariffs. "During the quarter, we saw proof in the wisdom of our Thailand manufacturing investment," Harley-Davidson CEO Matt Levatich said April 23 on a first-quarter earnings call. "The tariff mitigation we realized allowed more competitive pricing and access to more customers." Other companies may similarly want to consider how they can mitigate newly imposed tariffs.

2. Raw material shortages. Political instability and plant shutdowns are likely to result in shortages of critical raw materials. The Resilience360 risk report cited as one example the world's supply of cobalt for lithium-ion batteries, used in a wide range of consumer products—from smartphones to electric vehicles.

According to the 2018 U.S. Geological Survey, 58 percent of worldwide production of cobalt in 2017 came from the Democratic Republic of Congo (DRC). The fact that so few mines produce this natural resource and that DRC has been linked to human rights abuses poses a high risk to supply chains that source this raw material.

Some companies are responding accordingly. Panasonic, for example, has announced plans to start developing cobalt-free automotive batteries. With certain raw materials being vulnerable to widespread disruption caused by demand spikes or production bottlenecks, other industries that depend on such resources may be forced to switch to other products.

3. Safety recalls. Quality issues in the pharmaceutical sector pose an especially high safety risk, as more drug companies source an increasing amount of active pharmaceutical ingredients from producers in developing economies, according to the Resilience360 report. Consider, for example, that several drug makers and sellers—including Teva Pharmaceuticals, Mylan, and CVS Health—are currently facing dozens of lawsuits after carcinogens were found in heart medications produced in a drug manufacturing facility in China.

"From a compliance point of view, what we see is a lot of focus on sourcing issues," Mirko Woitzik, a senior risk intelligence analyst at DHL Resilience360, tells CW. Firm are increasingly aware it's not always enough to work with just Tier 1 suppliers, but they also need more transparency down the line concerning who their most critical suppliers are sourcing from, and how compliant they are with safety risk, he says.

4. Climate change risk. Over the long term, climate change will continue to bring more frequent and severe weather patterns—droughts, flooding, tropical storms, wildfires, volcano eruptions and earthquakes—with wide-ranging and devastating effects

on global supply chains, according to the report.

As just one example, continued record-low water levels on Germany's Rhine River, which serves as a main conduit for several manufacturers, will continue to delay shipments and increase operational costs by hundreds of millions of dollars as companies are forced to turn to more expensive road or rail transport alternatives. Some companies, however, are finding ways to safeguard against this risk. Steelmaker Thyssenkrupp, for example, told Reuters that it's exploring alternative modes of transport and barge modernizations, and that it's expanding storage and reception facilities. Other companies may want to consider similar alternatives.

When it comes to natural disasters, certain regions of the world pose a significantly higher risk than other areas: Earthquakes, volcanic eruptions, and tropical storms are commonplace in Asia Pacific, where most countries sit along the Pacific Ring of Fire. Such natural disasters are also a common occurrence in Latin America, particularly in Chile, Peru, Ecuador, Nicaragua, and Guatemala, according to Resilience360. These high-impact events commonly wreak havoc on supply chain operations in these parts of the world, due to power outages, flight cancellations, port closures, and cargo ship groundings. So, companies should have risk mitigation plans already in place to plan in advance for such disasters.

5. Tougher environmental regulations. To counter the impact of climate change, authorities around the world have started to introduce stricter environmental regulations and step up their enforcement efforts, including new rules governing emissions and the imposition of new carbon taxes. "Some of the most significant effects of these policies are expected in China, where strict rules have been introduced to reduce emissions from the burning of coal, including enforced production shutdowns and plant closures," Resilience360 said.

6. Economic uncertainty. The global trade war, uncertainty over Brexit, and tougher environmental regulations could all become driving factors in bringing insolvencies to the forefront of supply chain risk management in 2019. "Supplier insolvencies are set to rise as small producers continue to be casualties of economic uncertainty and structural change," Resilience360 said in the report. This means many lower tier suppliers may be forced to adapt their business models, or companies may have to seek alternative suppliers in some situations.

7. Cargo theft. Because goods are typically stolen while in transit, cargo theft mostly threatens the supply of electronics and consumer goods, and, thus, hotspots for cargo theft are typically places where goods transit between supply chain sites. "Metropolitan areas in countries like Mexico, Brazil, Chile, Venezuela, United Kingdom, Germany, and Italy continued to be explicit hot spots for cargo theft," Resilience360 said.

Region-by-region, hotspots for cargo theft in Europe are in Germany, Belgium, and the Netherlands. In Latin America and the Caribbean, hotspots for cargo theft include major ports in Costa Rica; Trinidad and Tobago; Colombia; Venezuela; Piura, Lima and Callao in Peru; Chile; Argentina; and Brazil. And in South Africa, the hijacking of cargo trucks and the rail networks is an especially common occurrence in the large metropolises and port cities of Johannesburg, Port Elizabeth, Durban, and Cape Town. In Africa, piracy continues to be a very real threat, particularly in the Gulf of Guinea, with cargo ships and tankers being primary targets.

Port congestion also pose a major supply chain risk, causing significant shipping delays. In some parts of the world—like China, India, and the Philippines—port congestion is predominately caused by adverse weather conditions, while in South Africa and Nigeria, war and terrorism-related incidents can result in port or ground transportation disruptions, sometimes preventing entry into, or exit from, a city's port, according to Resilience360. In other parts of the world, widespread strikes, protests, and riots are the cause of disruption, such as what's happening in France with the "Yellow Vest" protesters.

8. Container ship fires. Several major container ship fires in 2018 and early 2019 highlight what continues to be a growing risk for maritime-dependent supply chains. Two high-profile examples include the Maersk Honam fire in March 2018 and the Yantian Express fire in January 2019. According to insurance company Allianz, numerous factors cause container ship fires, including "the adequacy of fire-fighting capabilities, ongoing problems with misdeclaration of cargo, salvage challenges and how long it can take to access ports of refuge."

Industrial fires and explosions, which tend to cause ripple effects on downstream manufacturing industries, should also be on the risk radar of supply chain leaders. In the Asia Pacific region, for example, short circuit faults, machine overheating, and carelessness in working areas are the common causes of industrial fires, according to Resilience360. Such incidents highlight how important it is to know what safety precautions are being taken in the plants and facilities within the supply chains.

9. Border battles. In the United Kingdom, looming uncertainty over post-Brexit trade policies creates questions as to what new tariff and customs regimes might look like, and how those new regimes may affect and potentially reorient U.K.-affiliated supply chains. "Companies face the immediate risk of increased costs and border crossing wait times, especially in the period where customs agents are adapting to new processes," Resilience360 said in the report.

Operationally, all supply chains dependent on U.K.-based suppliers or EU-U.K. lanes will be forced to develop contingency plans. "Companies are taking action already because they can't just wait and see," Woitzik says. Many companies are shifting not only their production but also their distribution facilities from the U.K. to mainland Europe, especially to the Netherlands, he says.

"We've also seen efforts in using alternate routes because of fears around port congestion," Woitzik adds. For critical goods, especially, companies may want to think about shifting to air and freight transportation between the U.K. and EU in case of port congestion, he says.

10. Drone risk in the aviation industry. "Airport disruptions related to air traffic safety are likely to become more frequent in 2019, and thus present a greater risk of disruption to aviation logistics operations," Resilience360 said. One of the hardest hitting incidents occurred in December 2018, when multiple drone sightings resulted in the closure of London Gatwick Airport, wreaked havoc on over 1,000 flights for over 33 hours. Airports all around the world, however, have also reported cases of near-misses with drones, including in the United States, Canada, China, France, New Zealand, and Poland. Air traffic controllers are the first line of defense and can play a risk-mitigation role by immediately reporting drone sightings over radio air traffic communication frequencies.

Conclusion

When thinking about the top 10 risks for 2019, how prepared are companies when it comes to mitigating supply chain risk? "Overall, companies are not very prepared," says Resilience 360 Chief Executive Officer Tobias Larsson. They don't often have an enterprise-wide view of their supply-chain risks.

Companies with a truly best-in-class supply chain risk management strategy are those that proactively plan for disruptions by using advanced predictive analytics to assess what disruptions could occur down the road. That way, when disruptions occur in the supply chain that demand an immediate response, the company and its customers will have thought about its strategy well beforehand so that they won't be caught off-guard.

"The main thing you can do is get information out on time," Larsson says. Giving your customers time to respond accordingly to supply chain disruptions helps develop customer relationships. "If you do it better than your competition, you can gain market share," he says. "Even if you're in tough situations, that's when the strongest companies thrive." ■

A look at the NIST Risk Management Framework

NIST's new framework offers direction in integrating cyber-security, privacy, and supply-chain risk management. **Jaclyn Jaeger** has more.

The National Institute of Standards and Technology recently published the final version of its latest Risk Management Framework, gifting companies across all sectors with a comprehensive new roadmap as they look to seamlessly integrate their cyber-security, privacy, and supply-chain risk management processes.

NIST published Risk Management Framework (RMF) 2.0—formally called NIST Special Publication 800-37 Revision 2—on Dec. 20, 2018, following a seven-month consultation and comment period. Importantly, RMF 2.0 provides cross-references to NIST's widely adopted Cybersecurity Framework (CSF) throughout the 183-page document, so that users of the RMF can see exactly where and how both frameworks align with one another.

Published in April 2018, the CSF has been widely adopted by many in the private sector as a yardstick against which companies measure their cyber-security practices relative to the threats they face. Cyber-security professionals, chief privacy officers, and even supply-chain risk managers can use RMF 2.0 in much the same way—by choosing the specific security and privacy controls that they need to implement within their own organizations. Moreover, the framework has been purposefully designed to be "technology neutral so that the methodology can be applied to any type of information system without modification."

One of the main objectives of RMF 2.0 is "to provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization," NIST said. Whereas earlier versions of the framework focused primarily on cyber-security protections from external threats, the new version has been enhanced with privacy risk-management processes "to better support the privacy protection needs for which privacy programs are responsible," NIST said.

Although RMF 2.0 principally focuses on managing information-security and privacy risk, supply chain risk management (SCRM) concepts that overlap with these risks are also specifically incorporated in several areas of the framework to help promote a more holistic approach to managing security and privacy risks.

Because of the increased reliance on third parties and commercial-off-the-shelf products, systems, and services, attacks in the supply chain are increasing. "Adversaries are using the supply chain as an attack vector and effective means of penetrating our systems, compromising the integrity of system elements, and gaining access to critical assets," NIST said.

Thus, RMF 2.0 incorporates SCRM processes with the overall objective, NIST said, "to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the [system development lifecycle]."

Ron Ross, a fellow with NIST and one of the report's authors, says "RMF 2.0 is the only framework in the world that integrates security, privacy, and supply-chain risks." While adoption of the RMF and CSF is mandatory only for federal agencies, many in the private sector can—and do—use it to enhance their own controls.

"They may just use it on a voluntary basis because they want to protect their company's assets, their information, their operations," Ross says.

"This is why we're trying to bring more discipline and structure to the whole area of security and privacy."

New 'prepare' step

In total, the framework includes seven steps, as well as a detailed summary of tasks and expected outcomes for each of those steps. "All seven steps are essential for the successful execution of the RMF," NIST said.

Among its most significant changes, RMF 2.0 includes a new "prepare" step—the first step in the framework outlining which activities are essential at the organizational and information-system levels to help manage security and privacy risks, including supply-chain risk.

NIST recommends using the tasks discussed in the prepare step to promote a consistent starting point to execute the RMF. The intent of this step, NIST said, is to leverage activities that security, privacy, and supply-chain programs already conduct "to emphasize the importance of having organization-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization."

As discussed in RMF 2.0, preparation tasks may include, for example:

» Assigning roles and responsibilities for organizational risk management processes;
» Establishing a risk-management strategy that includes a determination of risk tolerance;
» Identifying the missions, business functions, and business processes the information system is intended to support;
» Identifying and prioritizing assets that require protection, including information assets;
» Conducting organization- and system-level risk assessments; and more.

"Risk assessments of the organization's supply chain may be conducted, as well," NIST said. How to document SCRM strategies may vary. At the organization and business-process levels, for example, SCRM strategies can be documented in the company's information-security program plan or in a separate business process-level SCRM strategy plan. For more guidance, turn to NIST's SCRM strategy template in SP 800-161.

The remaining six steps, which NIST describes in significant detail, are:

» Categorize the system and the information processed, stored, and transmitted by the system based on an impact analysis.
» Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
» Implement the controls and describe how the controls are employed within the system and its environment of operation.
» Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
» Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, and other organizations is acceptable.
» Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

For cyber-security professionals, chief privacy officers, and supply-chain risk managers seeking additional guidance, "we're working on a companion publication, which should be out in a couple of months," Ross says. That publication is NIST Special Publication 800-53, a catalog of security and privacy controls to be used alongside the Risk Management Framework. ■

Galvanize

7 steps to improve supply chain visibility

RISK IS INEVITABLE IN ANY INDUSTRY

The only way you could completely eliminate supply chain risk would be to avoid working with external business partners, manufacturers, suppliers, and other third parties—and how realistic is that?

One of the main challenges is that supply chains have gone global and digital. While innovations like cloud-based data systems, the internet of things (IoT), machine learning, and robotic process automation have all changed many processes for the better, they've also complicated risk management.

One of the biggest risks to an organization is their lack of visibility into third parties like suppliers. In fact, a third of organizations don't actually know how their suppliers are performing[1]—does yours? Here are seven ways to improve your supply chain visibility for a better risk management program.

The biggest challenge for global supply chain executives in 2018 was visibility (21.8% of respondents).[2]

PROCESS AND TECHNOLOGY IN THE SCRM LIFECYCLE

With improved processes and dedicated technology, you can assess a third party's performance at each stage of the supply chain risk management (SCRM) lifecycle.

01

Create a standardized, automated onboarding process

From pre-screening to collecting required documentation (e.g., insurance, certifications), following a standard onboarding process ensures that you're not missing any critical requirements. It also shows that you and your vendor or supplier are prepared to start doing business together. You'll want to first define the process and use your software to standardize the workflow so that you're consistently collecting the right information from your suppliers.

As part of your onboarding, you'll want to create a central repository of suppliers. By tracking the vendor through key milestones you'll be able to see, at any time, where a third party is in the onboarding process. Your process should include an easy way for business units and/or procurement to add new requests with a simple online form. Ideally, you'll use a tool that will automatically notify you, and kick-off an automated onboarding workflow, when a new supplier request is added.

02

Create a risk profile for each supplier

Risk profiles allow you to define your relationship and understand the products/services a supplier will provide—and how essential they are to your organization. It will also define what type of physical, systems, and data access to give the supplier.

Categorization through risk profiling helps you identify what type and level of assessment is required for the new vendor, so you can focus on your high-risk supplier(s).

[1] **CIPS,** *2019: Third of firms "don't know how suppliers perform"*
[2] **Statista,** *2019, Biggest supply chain challenges worldwide 2017-2018*

03

Use risk and controls assessments

Once you understand the risk a supplier presents, you'll need to check that the proper controls are in place to manage that risk, and that they're operating effectively. Those controls can be part of a larger framework.

There's no need to reinvent the wheel; you can align to best-practice industry control frameworks (e.g., NIST, ISO, CSA) to support your assessment process. Organizations often use more than one industry framework to define assessment questions. Software with a harmonized content library can make things much easier, by letting suppliers complete a single assessment.

04

Have a remediation management plan

It's not uncommon to find an issue when onboarding suppliers during your assessments (in fact, if you never find a single issue, that in itself is a risk!). Knowing how you want to address your findings to keep the onboarding process going is critical. The right software will automate your workflows so that you can either remediate, create compensating controls, or accept the risks to save you time and increase accuracy.

05

Regularly review risks and contracts

Now that you've remediated your issues, you'll want to consider how well your suppliers are performing against their contracts. You have to regularly review contracts (commonly done on a monthly or quarterly basis) to monitor third-party performance and stay ahead of renewals or expirations. Because poorly managed contracts are a source of both increased risk and revenue loss, as are manual contract management methods.

06

Mandate ongoing supplier monitoring

It's not just the contract that requires a regular check-in. That supplier you vetted a year ago (and haven't checked back on) could put you in danger of a compliance violation or paralyze your supply chain today. Ongoing monitoring can be accomplished in a number of ways, but some common methods include:

+ Automating the scheduling of follow-up assessments based on the risk level of a supplier. (A low-risk supplier may be scheduled for re-assessment every three years, while a critical supplier might require quarterly reviews.)
+ Using rule-based automation to trigger assessments when thresholds are breached or related events discovered (e.g., a significant incident identified with a related third party).
+ Integrating third-party intelligence feeds that provide ongoing monitoring alerts for significant changes to a supplier's/vendor's risk ratings (e.g., credit ratings, IT security risk ratings), new appearances in adverse media or on government watch lists, or the filing of public records involving them.

07

Define a supplier offboarding process

You may end a relationship with a third party for a number of reasons, but it isn't as simple as just stopping your orders. You'll need an offboarding strategy that includes finalizing payments, disabling supplier access to data, and more. Just like your onboarding process, the offboarding process can be managed through your software and partially (if not almost totally) automated, to ensure you don't miss anything.

GETTING STARTED WITH SUPPLY CHAIN RISK MANAGEMENT

Regulatory requirements, stakeholder expectations, and organizational goals and risks will always shift over time. By following the SCRM lifecycle and implementing a software solution that can quickly adapt to changes, you'll increase visibility into your supply chain and make processes easier and more efficient for everyone involved. ***Learn more at wegalvanize.com/highbond***

Blockchain Network welcomes Volvo

The Responsible Sourcing Blockchain Network announced its digital supply chain for cobalt has moved beyond pilot phase and is progressing toward use in live production computing environments from spring 2020, just as Volvo joins. **Jaclyn Jaeger** has more.

The Responsible Sourcing Blockchain Network, a blockchain network committed to strengthening human rights and environmental protection in mineral supply chains, announced that its digital supply chain for cobalt has moved beyond pilot phase and is progressing toward use in live production computing environments from spring 2020, just as Volvo joins as its newest member.

Built on the IBM Blockchain Platform, the Responsible Sourcing Blockchain Network (RSBN) and its pioneering participants are working to build an open, industry-wide blockchain platform that provides for the traceability and verification of responsible sourcing practices from mine to market, including the end-to-end supply chains. The solution is designed in such a way that it allows companies of

any size in the mining industry to contribute data in a secure and permissioned way.

Traditionally, miners, smelters, and consumer brands have relied on third-party audits and laborious manual and paper-based processes to establish compliance with industry standards. The blockchain network allows the secure and permissioned sharing of information to enable visibility into the end-to-end supply chain in real time. RCS Global consistently assesses each participating company against responsible sourcing requirements set by the Organization for Economic Cooperation and Development (OECD) and relevant industry bodies, like the Responsible Minerals Initiative (RMI) Blockchain Guidelines.

Focus industries include, but are not limited to, automotive and consumer electronics, including their supply chains and the mining sector. A governance board representing members across these industries is being formed to help further ensure the platform's growth, functionality, and adherence to good practice principles.

"We are setting in motion a process of mainstreaming responsible sourcing practices across major industries," said RCS Global Group CEO Nicholas Garrett. "We've reached significant new milestones as we've moved beyond testing, proving the merits of this coupled technology and assurance model can extend to a wide range of participants across every tier of the supply chain and to other minerals."

Founding RSBN members include Ford Motor Company, Volkswagen, LG Chem, and Huayou Cobalt. Volvo Cars announced it on Nov. 6 that it would be joining this cross-industry network as its newest member. More partners from the auto, tech, and mining sectors are expected to join this year.

"The early addition of Volkswagen Group, and now Volvo Cars, to this collaboration confirms that blockchain technology coupled with responsible sourcing assurance can help address critical sustainability issues impacting the entire industry," Garrett added.

Volvo will be the first company in the consortium to fully apply the RSBN solution in its LG Chem supply chain from spring 2020. The automaker said it also plans in the future to apply RSBN to other key minerals found in its batteries, including nickel and lithium.

"We have always been committed to an ethical supply chain for our raw materials," said Martina Buchhauser, head of procurement at Volvo Cars. "With blockchain technology we can take the next step in ensuring full traceability of our supply chain and minimizing any related risks, in close collaboration with our suppliers."

> "As a founding member of the network, we are pleased that the project is moving to an operational phase. This will further strengthen the human rights protection and responsible sourcing efforts in mineral supply chains."
>
> Lisa Drake, VP or Global Purchasing & Powertrain Operations, Ford

Volkswagen, too, has been working with relevant battery suppliers to address the need for supply chain due diligence and is now aiming to significantly increase its supply chain mapping and auditing activities for key battery mineral supply chains. Through the RSBN, and other initiatives, Volkswagen is utilizing technology toward securing better supply chain traceability and transparency and to connect this information with the sustainability performance of supply chain partners.

As Ford prepares to launch its global all-electric Mustang-inspired SUV next year, the RSBN becomes an important tool to strengthen transparency and visibility into its global mineral supply

"We have always been committed to an ethical supply chain for our raw materials. With blockchain technology we can take the next step in ensuring full traceability of our supply chain and minimizing any related risks, in close collaboration with our suppliers."

Martina Buchhauser, Head of Procurement, Volvo Cars

chain. Expanding this network beyond cobalt to other battery minerals will compound the RSBN's positive impact on human rights protection and labor practices.

"As a founding member of the network, we are pleased that the project is moving to an operational phase," said Lisa Drake, vice president of global purchasing and powertrain operations at Ford. "This will further strengthen the human rights protection and responsible sourcing efforts in mineral supply chains. This becomes even more important as we start to launch our next generation of all-electric vehicles starting next year."

Making progress

In initial testing, the RSBN blockchain demonstrated how cobalt produced at Huayou's industrial mine site in the Democratic Republic of Congo (DRC) could be traced through the supply chain to LG Chem's cathode and battery plant in South Korea and then to its destination, a Ford plant in the United States. An immutable audit trail captured on the platform delivered corresponding data providing documentation for the initial ethical cobalt production, its maintenance, and its ethical provenance from mine to end-manufacturer.

This progress comes at a crucial time for the industry. According to a recent supply chain risk report by DHL Resilience360, there will be a shortage in critical raw materials, including cobalt, presenting a high risk to supply chains that source this raw material. "Battery minerals like cobalt are foundational to a number of industries, from automakers to consumer electronics and smartphone manufacturers," said Manish Chawla, global managing director of chemicals and petroleum/industrial products industries at IBM.

Moreover, 58 percent of worldwide production of cobalt in 2017 came from the DRC, according to the 2018 U.S. Geological Survey. The fact that so few mines produce this natural resource and that DRC has been linked to human rights abuses.

"The Volkswagen Group has set itself a goal of full transparency in the critical supply chains of our parts and products, which includes cobalt," said Ulrich Gereke, head of strategy for Volkswagen Group procurement. "Due to the particular complexity of many critical supply chains, such transparency goals represent a difficult challenge."

"Thus, with the help of new technologies and digital solutions, the Volkswagen Group is continually working toward securing better supply chain traceability and transparency and to connect this information with the sustainability performance of supply chain partners," Gereke said. "In this manner, we will be able to identify sustainability risks at an early stage and improve our ability to react to them in a timely manner. The Volkswagen Group encourages other business partners to join the network."

Moving forward, the RSBN said its plan is to extend into other battery metals, including lithium and nickel. The platform is also actively working to progress the solution to support tracing other common metals, including 3TG metals—tungsten, tantalum, tin, and gold. ■

U.K. grocers slammed for supply chain worker abuse

In an effort to cut costs and raise revenue, U.K. supermarkets are endangering employees with such abuses as a lack of toilets, unsafe drinking water, and more, reports Oxfam. **Neil Hodge** explores.

The "relentless" drive by U.K. supermarkets to cut costs and boost profits is fueling poverty, abuse, and gender discrimination in their supply chains in developing countries, says Oxfam in its latest report.

The British charity says poor pay and harsh working conditions are "common" on farms and plantations that supply tea or fruit to global supermarkets including Lidl, Aldi, Sainsbury's, Tesco, and Morrisons.

The research, set out in a series of reports, includes in-depth interviews with workers in India and Brazil and a survey of workers in five other countries. And they catalogue some awful details.

Interviews with workers on 50 tea plantations in Assam that supply Aldi, Morrisons, Tesco, and Sainsbury's (Walmart, which owns Asda, would neither confirm nor deny that it sourced from the region) revealed cholera and typhoid are prevalent because workers lack access to toilets and safe drinking water.

Half the workers questioned receive ration cards from the government because wages are so low. Women workers, who are often in the lowest paid—but most labor-intensive—jobs, regularly clocked up 13 hours of back-breaking work a day for little reward. Oxfam found that of the 79 pence (U.S. $1) paid by shoppers for a pack of 100g black Assam tea in the United Kingdom, supermarkets and tea brands receive 49 pence (U.S. $0.6) while workers collectively receive just three pence (U.S. $0.04).

According to the charity, if workers on these tea estates received just five pence (U.S. $0.06) more of the retail price, they could be paid a living wage.

Meanwhile, women with children working on fruit farms in Northeast Brazil said they were forced to rely on relatives or government support to feed their families outside the harvest season because wages were so low. Workers also reported developing allergies and serious skin diseases as a result of using pesticides and other chemicals without adequate protection on grape, melon, and mango farms that supply supermarkets including Lidl and Sainsbury's (and previously Tesco and Morrisons).

A separate Oxfam survey of over 500 workers on farms and plantations in the Philippines, Ecuador, Costa Rica, Peru, and the United States found three quarters of workers said they were not paid enough to cover basic needs such as food and housing. Over a third said they were not protected from injury or harm at work and were not able to take a toilet break or have a drink of water when they needed it.

"Despite some pockets of good practice, supermarkets' relentless pursuit of profits continues to fuel poverty and human rights abuses in their supply chains," said Oxfam's ethical trade manager Rachel Wilshaw in a statement.

"Supermarkets must do more to end exploitation, pay all their workers a living wage, ensure women

"Having robust compliance processes in place and a transparent view of business relationships can help to identify whether suppliers, customers, or other partners are involved in modern slavery, corruption, fraud, and other nefarious activities."

Chris Laws, Head of Product & Strategy, Dun & Bradstreet

get a fair deal, and be more transparent about where they source their products," she added.

Oxfam's scrutiny of the U.K.'s top six supermarkets is part of its global Behind the Barcodes campaign, which tries to bring improvements to the working lives of unskilled laborers working in the food industry's supply chain through advocacy, engagement and—to some extent—"naming and shaming."

According to Oxfam's scorecard rating, based on an examination of supermarkets' policies, practices, and the behaviors in place to protect farm workers, Lidl is the U.K.'s worst-performing major supermarket. Tesco is top—though with a score of just 38 percent (up from 23 percent last year), the ranking is hardly a ringing endorsement.

In response, Peter Andrews, head of sustainability at industry body the British Retail Consortium, which represents all the supermarkets mentioned in the Oxfam report except for Tesco, said: "Supermarkets in the United Kingdom are spearheading actions aimed at improving the lives of the millions of people across the globe who contribute to the retail supply chain. Our members are working hard to address existing injustices and continue to collaborate internationally with NGOs, business groups, and government on this vital issue."

A spokesperson for Tesco said in an emailed statement: "We know there is always more to do and we are working collaboratively with NGOs, trade unions and others to improve wages in the key produce, tea and clothing sectors and ensure working conditions are fair."

Chris Laws, head of product & strategy at ratings agency Dun & Bradstreet, says Oxfam's research has "shone a spotlight" on the problem of how business is conducted within the supply chains of the country's biggest supermarkets.

"The call for more supply chain transparency to identify and address risks has never been louder," said Laws. "Having robust compliance processes in place and a transparent view of business relationships can help to identify whether suppliers, customers, or other partners are involved in modern slavery, corruption, fraud, and other nefarious activities," he added.

The U.K.'s Modern Slavery Act, which requires large companies to make a statement about what steps, if any, they are taking to tackle slavery in the supply chain, has made organizations more conscience of the need to monitor violations of workers' rights (though not necessarily more effective in tackling such abuses).

The United States has been trying to tackle the problem for nearly 90 years. Section 307 of the Tariff Act of 1930, for instance, prohibits the importation of merchandise mined, produced, or manufactured, wholly or in part, in any foreign country by forced or indentured child labor. The U.S. Department of Labor also produces an annual publication to highlight goods that have been produced using forced and/or child labor and the countries where this takes place.

In its 2018 List of Goods Produced by Child Labor or Forced Labor, the Labor Department lists 148 goods from 76 countries as being produced with forced or child labor. ■

Three steps to a supermarket scorecard:

1. We examined supermarkets' policies and practices

2. We looked for behaviour that protects the rights of workers, farmers and women and gave each supermarket a score out of 100%

3. The higher the percentage, the better your supermarket checks out on human rights – but all six still have a long way to go.

	2018	2019	
TESCO	23%	38% ↑15%	⌄
Sainsbury's	18%	27% ↑9%	⌄
ASDA	17%	23% ↑6%	⌄
ALDI	1%	19% ↑18%	⌄
Morrisons	5%	16% ↑11%	⌄
LIDL	5%	9% ↑4%	⌄

Galvanize

You're only as strong as your weakest vendor

Software to manage the entire vendor risk process.

From third-party onboarding, assessment, and remediation, to performance monitoring and ongoing review, our ThirdPartyBond software by Galvanize manages the entire process.

See how ThirdPartyBond can work for you.

wegalvanize.com/vendor-risk-management >