WINTER 2018
www.bdo.com

THE NEWSLETTER FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

BDO KNOWS: GOVERNMENT CONTRACTING

IN AN UNCERTAIN TIME, CONSIDER ESOPS: PART 2

By Jay Powers, Christopher Carson

In the Summer 2017 edition of BDO Knows Government Contracting, we broke down why government contractors might consider Employee Stock Ownership Plans (ESOP) as a way to incentivize company partners and encourage cash-flow. To better understand an ESOP in practice, consider a scenario where a government contractor owned by two individuals is looking for liquidity while continuing to operate the day-to-day functions of the business.

CLIENT AND MOTIVATION

The two owners are specifically concerned about getting some ownership into the hands of younger management team members, who will drive the business moving forward. However, the owners recognize the importance of the culture of the business and the key relationships they have developed with their client. Unlike an outright sale to a competitor or private equity firm, an ESOP guarantees the culture the company has built will stay intact, while the current owners can still control the board and run the business, if they so desire.

As mentioned in Part 1 of this article, there are a number of advantages for implementing ESOPs for government contractors. Similar to employer 401(k) contributions, ESOP contributions are allowable costs under the Federal Acquisition Regulation (FAR), even

Ask the Pros

If you have a question—large or small—or are searching for a resource, you can count on our team to help you get on the right track with timely knowledge and thorough insights. Our practice combines extensive experience in government contracting work with deep understanding of the latest technical, compliance, accounting, regulatory and business matters important to contractors.

Go ahead, ask one of our pros.

CHRISTOPHER CARSON
National Government Contracting Practice Lead, Audit Partner
703-770-6324 / ccarson@bdo.com

ERIC JIA-SOBOTA
National Leader, Government Contracts and Grants Advisory Services
703-770-6395 / esobota@bdo.com

JOE BURKE
Partner, Transaction Advisory Services
703-770-6323 / jburke@bdo.com

STEPHEN RITCHEY
Audit Partner
703-770-6346 / sritchey@bdo.com

JEFF SCHRAGG
Tax Partner
703-770-6313 / jschragg@bdo.com

DEREK SHAW
Director
703-336-1501 / dshaw@bdo.com

ANDREA WILSON
Managing Director, Grants Advisory Services
703-752-2784 / aewilson@bdo.com

Read more ▶

CONTINUED FROM PAGE 1

ESOPS: PART 2

though payments may be designated for repayment of principal, and interest, of the underlying loans. Further, government contractors structured as S Corporations may benefit from the fact that any tax liability flows through to the ESOP Trust, which pays no income taxes. This benefit provides an important source of cash flow for the pay down of the ESOP loan. Finally, ESOP-owned government contractors that otherwise meet the applicable revenue or headcount limitations will be eligible for "small business" status and retain the associated competitive advantages.

Revenue Range: $25 Million

EBITDA Range: $3.0 Million

Transaction Value Range: $18 Million

Financing: Initially structured with approximately 25 percent senior (bank) note and 75 percent seller notes. The seller notes are structured to pay out a total rate of return commensurate with the current market requirements of mezzanine providers (since structured as subordinated debt to the senior note), and usually include detachable warrants.

Post-ESOP Value of Company: $2.7 Million (approximately 15 percent of pre-ESOP Value).

Value of Warrants: 25% of increase in value above $2.7 Million

Seller Take Home: Sellers receive $4.5 Million cash up front, $13.5 Million over 10-15 years plus interest, and 25 percent upside over post-ESOP value (approximately $3.8 Million if company value returns to $18 Million—very possible because of repayment of debt every year).

Effect on Company Cash Flow: While the company is levered post-transaction, if constructed as an S Corporation ESOP, there is more cash to service the debt and fund company growth – approximately $1.2 Million a year of tax savings with EBITDA of $3.0 Million.

Management Incentive Plan (MIP): A management incentive plan would reward key management team members outside of and in addition to the ESOP. The pool would be equal to a percentage of the equity of the company, and participation is usually limited to key management team members, but can be changed at any time.

Possible Issues of the ESOP for a Government Contractor: Negotiation of value and senior financing could be challenging, as the trustee/valuation firm and senior lender may have concerns about the company being too dependent on one client. However, if the owners plan to stay with the company and continue these relationships, and this fact is properly communicated, this may not be an issue, particularly with banks with a market presence in the government contracting industry. Repurchase obligation must always be a concern of business owners when considering an ESOP, but this can be somewhat mitigated for government contractors through the cost recovery of the ESOP contributions and S Corporation status.

Overall Impact of ESOP for Government Contractors: For business owners seeking liquidity and diversification while also continuing to run the day-to-day operations, there is no better option than ESOP. This is important for many government contractors because of the important relationships built with their government customers, and the unique corporate cultures best suited to support them. Owners getting closer to retirement can begin the transition of relationships to younger, key management team members while also rewarding them with ownership in the company. Tax incentives also make the ESOP enticing to both the company and owners.

Although each company is different, and potential issues must always be addressed, an ESOP offers a very flexible, smooth exit strategy for business owners who value company culture and legacy.

Jack Southers, Senior Associate, contributed to this article.

Jay Powers is the National Practice Leader for BDO's ESOP Transaction Services and may be reached at jpowers@bdo.com.

Christopher Carson is the Assurance Practice Office Managing Partner of BDO's Center of Excellence for Government Contracting and Government Contracting Practice Leader. He may be reached at ccarson@bdo.com.

Read more ▶

MEET THE NEW MANAGING DIRECTORS

Kathleen Kulp

Wiley Wright

Paul Jan Zdunek

This fall, we're glad to welcome several new members to BDO's Government Contracting practice. **Get to know our newest managing directors.**

Q: Tell us a bit more about your background:

Kathleen Kulp (KK):
I graduated from Bloomsburg University with a major in speech communication and organizational development. Prior to joining BDO, I was a Senior Principal with QuintilesIMS focusing on systems integration for pharma manufacturers. I've spent the last 20 years in consulting.

Wiley Wright (WW):
I began my public accounting career doing traditional audit and tax work. After testifying for a client in a government contract dispute, I focused my next 30 years consulting on compliance issues and providing expert testimony in disputes.

Paul Jan Zdunek (PJZ):
I began my career as a conductor and have two music degrees: a Bachelor of Music in composition from The Peabody Institute of Johns Hopkins University and a Master of Music in conducting from The Cleveland Institute of Music. After a decade of conducting, I realized my real interests were in executive management. Now I have an MBA from the Peter F. Drucker School of Management at Claremont Graduate University, and have spent the last 15 years helping facilitate turnarounds for troubled organizations.

Q: What are some specific milestones in your career? What challenges have you learned from?

KK: My first entry into consulting was with CSC, a consulting firm. I was coming from the automotive industry and had no technical or consulting experience. I attended an 8-week intense training program that was supposed to prepare me for coding and consulting. I hated it, yet 20 years later I'm still in consulting and in a business systems role. The point is, you have to work through the things you think you don't like because you never know where they will lead. By chance, I ended up with a large pharmaceutical client and over the years I've worked with that client numerous times.

WW: My first milestone was transforming my work from traditional to specialized services. My second milestone was my successful 30-year relationship with the Department of Justice, providing expert testimony. My third milestone was earning recognition for a national top-50 jury verdict in a lost profits case.

PJZ: My biggest "ah-ha" moment took place during my time at the conservatory listening in on colleagues' practice sessions: "Being excellent at what you do is not enough, it's a given. You have to find what differentiates you from the rest of the pack – that differentiator is what ultimately will make you wildly successful."

Q: How have you developed technical and industry knowledge to advance in your career?

KK: The majority of what I know I've learned from doing. Having many clients afforded me the opportunity to see how companies approach a common task of contracting. Most large pharma manufacturers use the same technology, but how they use it is different—it's a different project every time. I also attend various conferences each year and keep in touch with previous clients, checking in on their progress and changes.

WW: For me it comes down to research, and connecting specific issues on cases.

PJZ: I develop new skills, knowledge and ways of doing things every day by remaining curious about everything around me, from new challenges I may face during a client's crisis, to conversations I overhear while standing in line at the grocery store.

Read more ▶

CONTINUED FROM PAGE 3

MANAGING DIRECTORS

Q: What advice would you offer young professionals?

KK: Talk to people—don't wait for someone to come to you. Be the first to initiate the conversation and have a strong handshake. First impressions matter. Don't answer a question you don't know the answer to. It's OK to say that you'll get back to someone with the right information.

WW: Out-prepare any adversary in a dispute setting and know all of the details.

PJZ: If you focus on consistently doing great work, your career will take care of itself.

Q: How did you come to be interested in what you do?

KK: It was an accident getting here, but over the years it has kept my interest because there's so much to learn. Just when you think you've got it, there's a change in the business approach. It also helps to work with people that you like to be around and can spend long days with. You can learn a lot from their experiences, and if they're excited, it can be contagious.

WW: My competitive nature led me here.

PJZ: I found out by chance that I was good at turning organizations around, and I loved doing it! It's like solving a jigsaw puzzle. When someone tells me, "that's impossible to solve," that gets my energies roaring and I can't wait to prove them wrong.

Q: What role did mentorship play in your advancement?

KK: I've had a few great mentors in many areas during my career. Some formal, but most informal, which I find can be better in some ways. You have to find the people you admire and emulate the behavior you see. You have to be the change.

WW: Mentorship provided the opportunity to testify early in my career.

PJZ: Mentorship, and most importantly building and utilizing my network, was and continues to be the key to my personal and professional career success.

Q: What's your personal motto?

KK: Live today, because tomorrow is not guaranteed.

PJZ: I have two mottos that drive me: "If you don't try for it, you're absolutely guaranteed not to achieve it." The second motto I borrow from business management and nonprofit guru Peter Drucker: "The only way to predict the future is to create it."

Kathleen is based in BDO's Philadelphia office, Wiley is based in BDO's Annapolis office, and Paul is based in BDO's Los Angeles office.

Other notable recent hires include Mark Baker, Ted Needham, Erin O'Shea and Jim Telesmanich as directors, and Geoffrey Merritt, Kathy Stnons, and Erin Wilkerson as senior managers.

Read more ▶

6 CYBERSECURITY QUESTIONS GOVERNMENT CONTRACTORS SHOULD ADDRESS

By Gregory Garrett and Karen Schuler

With cyberattackers growing increasingly sophisticated in their methods and the number of data breaches on the rise, it's no wonder that cybersecurity is top of mind for both the public and private sectors. In fact, the numerous attacks in recent years have been serious and costly enough to prompt action at the federal level.

On May 1, the Trump administration released an executive order mandating that all U.S. federal government agencies plan, develop and submit formal cybersecurity risk management plans to help safeguard their sensitive information and controlled unclassified information (CUI). This new cybersecurity EO is designed to promote cyber risk mitigation across the entire government by holding each agency head personally responsible for network protection and requiring all agencies to modernize their information technology systems. In addition to the cybersecurity EO, each agency is also expected to use the National Institute of Standards and Technology's Cybersecurity Framework to enhance its controls and management of CUI.

The government is also requiring government contractors to be held accountable to similar cybersecurity standards, dictated by the NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." NIST SP 800-171 provides 109 individual controls categorized under 14 families of information security requirements designed to help companies control the security of their CUI. This set of cybersecurity requirements is soon to be implemented across government contractors via a new final rule to the Federal Acquisition Regulation, which is an expansion of the current U.S. Department of Defense's Defense Federal Acquisition Regulation Supplement implemented in June 2016.

With these additional regulations on the horizon, it's not surprising that many government contractors feel overwhelmed; after all, they must now comply with several new requirements on top of the numerous industry-specific and international cyber standards, such as ISO 27001, already in place. As a result, many government contractors are experiencing numerous pain points related to the implementation of cybersecurity information governance, risk management and compliance.

Based on our discussions with more than 100 government contractors in recent months, we have outlined the top six cybersecurity questions they should address below.

Read more ▶

CONTINUED FROM PAGE 5

CYBERSECURITY QUESTIONS

1 How can government contractors accurately and cost-effectively assess their cybersecurity compliance according to NIST SP 800-171?

First, it is important to understand that NIST SP 800-171 is a set of guidelines established to help companies protect their CUI and DOD covered defense information (CDI) in nonfederal systems and organizations. CUI is a result of the Obama administration Executive Order 13556, issued in November 2010. The CUI system aims to standardize and simplify how the government handles unclassified information that requires safeguarding. There are 22 approved CUI categories of information, covering everything from agriculture, transportation and energy to defense technical drawings and product specifications provided by federal government agencies to government contractors.

Second, according to NIST, there are two classifications of security requirements: basic and derived. The basic security requirements are obtained from the Federal Information Processing Standard 200, which provides high-level fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the detailed security controls contained in NIST Special Publication 800-53.

Third, for a government contractor to ensure it receives an accurate and cost-effective assessment of its cybersecurity capabilities in comparison to the NIST SP 800-171 guidelines, it should competitively evaluate and select an independent professional services company with the ability to perform a high-quality and timely cyberrisk and gap assessment.

Currently, it appears that many government contractors do view the NIST 800-171 guidelines as a mandatory rule that requires full and strict compliance. It is expected that the new DFARS 252.204-7012 cybersecurity and information security management system will be treated in the same manner as the six current major contractor business systems: accounting, cost estimating, material management and accounting, government property management and earned value management.

2 What actions do U.S. government contracting officers plan to take if government contractors fail to comply with the DFARS 252.204-7012 (NIST SP 800-171 compliance requirement) after the Dec. 31, 2017, deadline?

So far, government contractors have been advised via updates from the DOD chief information officer that the Defense Contract Management Agency may request a copy of their system security plan (SSP) for purposes of evaluation for compliance with the NIST SP 800-171 requirements and that the Defense Contract Audit Agency may audit their related information security management systems' cost.

Concerns to consider:

- Currently, neither the DCAA nor the DCMA has the necessary cybersecurity expertise to assess the contractor's compliance with the standard. Without certified information system security professionals, certified information technology auditors or the like, they cannot accurately evaluate government contractors' SSPs to fairly assess their compliance with NIST SP 800-171.
- If the federal government decides to outsource the SSP evaluation to assess compliance with NIST SP 800-171, it is imperative to ensure that the selected companies are free of organizational conflicts of interest and personal conflicts of interest.
- If a government contractor is noncompliant with all or part of NIST SP 800-171, then the government contracting officer will have to decide on a number of actions. He or she can:
  - Withhold contractor payments up to 20 percent;
  - Issue a stop work order;
  - Issue a suspension of work; or
  - Terminate the contract for default.

3 How should government contractors pay for this additional cybersecurity compliance expense?

The DCAA has not yet provided specific guidance on how the new cybersecurity compliance-related expenses will be audited. Nevertheless, these costs will likely be audited in a similar manner to the six existing DFARS contractor business systems. Compliance-related business expenses may be categorized as a direct or indirect cost, depending on the contract requirements and the contractor's accounting system. Often, these DFARS contractor business system requirements are considered indirect costs. Thus, if these cybersecurity management system-related compliance costs are charged as indirect costs, properly allocated and considered fair and reasonable in both nature and amount, they should be deemed as allowable costs.

4 Do I have to purchase cybersecurity liability insurance?

Currently, the FAR and DFARS do not require government contractors to purchase cybersecurity liability insurance.

Concerns to consider:

- If a government contractor does purchase cyber liability insurance, will the cost of the insurance be considered as an allowable cost on a government contract?

Read more ▶

CONTINUED FROM PAGE 6

CYBERSECURITY QUESTIONS

- How much cyber liability insurance will be considered sufficient by the federal government and deemed an allowable cost?
- If a government contractor experiences a cyberattack that results in a network breach and its insurance provider denies some or all of the security-related breach remediation costs, will costs, if fair and reasonable in nature and amount, be deemed an allowable cost on a government contract?

5 Will prime government contractors be held contractually responsible and financially liable for cyber-related damages caused by their subcontractors and/or third-party partners' failure to comply with NIST SP 800-171?

The FAR states that prime contractors are responsible for the selection, administration and performance of their subcontractors.

Concerns to consider:

- The contract between prime contractor and a subcontractor is a commercial contract. Subcontractors have no privity of contract with the government. Often, prime contractors do not communicate all the appropriate government requirements to their subcontractors.
- Prime contractors often attempt to contractually transfer all responsibilities and financial liabilities to their subcontractors.

6 How can government contractors staff and retain high-quality cybersecurity talent to meet the increasing number of government information security compliance standards when considering the highly competitive marketplace and global shortage of cybersecurity professionals today?

The recruiting, staffing, training and retention of cybersecurity talent is a significant challenge for nearly every organization. The global shortage of experienced cybersecurity professionals is expected to increase over the next three to five years. Thus, the need to create the right balance of cybersecurity employees, tools and managed outsourced services becomes vital to all public and private organizations, especially for small to midsize companies.

SUMMARY

As government contractors are required to comply with new U.S. regulatory requirements every year, they are also experiencing a rise in compliance-related costs. Many government contractors will sometimes decide to defer them to see if the government will enforce the new guidelines. If they are enforced, contractors will often wait to see how much the penalties are — and if they are greater than the cost of compliance — to decide whether they should bear the additional expenses.

Government contractors often find themselves facing a dilemma: They must figure out the best way they can properly safeguard their CUI and ensure compliance with the NIST SP 800-171 guidelines, while continuing to remain competitive in the federal marketplace and achieve a fair and reasonable return on investment.

*Originally **published** on Law360.*

Gregory A. Garrett is head of international cybersecurity at BDO USA LLP in Washington, D.C. Previously, he was head of cybersecurity for the UIC Corporation and Blue Canopy Group LLC, managing director for Navigant Consulting Government Services, and chief compliance officer, chief information security officer and vice president and general manager of program management for Lucent Technologies Inc. He may be reached at ggarrett@bdo.com.

Karen Schuler is a partner in BDO's Washington office and head of the information governance practice. She is a former member of the U.S. Securities and Exchange Commission's forensic team. She may be reached at kschuler@bdo.com.

Read more ▶

GOVERNMENT CONTRACTORS: PREPARE FOR THE NEXT NATURAL DISASTER

By Steven Shill, Patrick Pilch, David Friend, and Clark Schweers

When it comes to natural disasters, it's not about *if* your supply chain will be impacted, it's *when*. No matter when or where disaster strikes, government contractors, regardless of industry, should anticipate and react accordingly.

For government contractors embedded in the life sciences industry, the consequences of supply chain disruption become a public safety concern. Like 1998's Hurricane George, Hurricanes Irma and Maria have underlined this concern. Following the storms, the FDA announced that the U.S. will likely experience drug shortages due to the natural disasters' residual impact on the drug manufacturing industry in Puerto Rico.

Nearly 10 percent of drugs prescribed in the U.S. are manufactured in Puerto Rico. Those include critically important products like treatments for cancer, HIV, and rheumatoid arthritis. More than 50 medical device plants are located in Puerto Rico, manufacturing more than 1,000 types of medical devices and employing 18,000 people. Only a small fraction of the power to the island has been restored, suggesting many drug and device manufacturers may not be fully online. FDA Commissioner Scott Gottlieb told *Reuters*, "It's unclear when they are going to be able to bring [production] up to full capacity."

On Oct. 20, the FDA released a **statement** outlining efforts in conjunction with federal and local agencies to rebuild the island, monitoring more than 40 medical devices manufactured there and working alongside pharmaceutical and medical device makers to expedite the process of getting factories back up and running.

Most recently, the FDA announced a significant shortage of IV fluids, particularly sodium chloride 0.9 percent injection bags, or saline bags. Although in shortage since 2014, "the situation in Puerto Rico has greatly exacerbated this supply issue," the FDA said on Nov. 17. In conjunction with the manufacturers of such products, the FDA said it's taking actions to temporarily allow the importation of IV saline products from abroad, encourage the growth of production at U.S. facilities, and streamline its review of new product applications that could help mitigate the shortage.

Read more ▶

CONTINUED FROM PAGE 8

NATURAL DISASTER

IMPACTS

Supply Chain

While many factories owned by large global pharmaceutical companies are running on generator power as backup, some of these plants may be the single manufacturer of a certain device type. The FDA said it is working with about 10 manufacturers, especially those manufacturing critical blood-related medical devices, which fall within this camp.

Outcomes & Reimbursement

If providers don't have access to the right drugs or devices, they could face **adverse financial impacts** including greater costs associated with delivering patient care through higher drug acquisition and personal costs. They may also have to prescribe an alternate drug that isn't as effective. That leads to implications for the effectiveness of care and potentially a hit to quality metrics, which would impact reimbursement under value-based arrangements, including those taking place under the Medicare Access and CHIP Reauthorization Act (MACRA). Providers who might be up against a shortage should work to understand what that could mean for their ability to attract investors.

Business Continuity Risk

The revenue disruption also poses an audit risk for pharmaceutical and medical device companies. If a plant is destroyed or not operating at full capacity, providers may be forced to turn to other suppliers for critical drug products, like cancer treatments, thus creating a going concern of business continuity issues for pharma and medical device companies.

BDO INSIGHTS

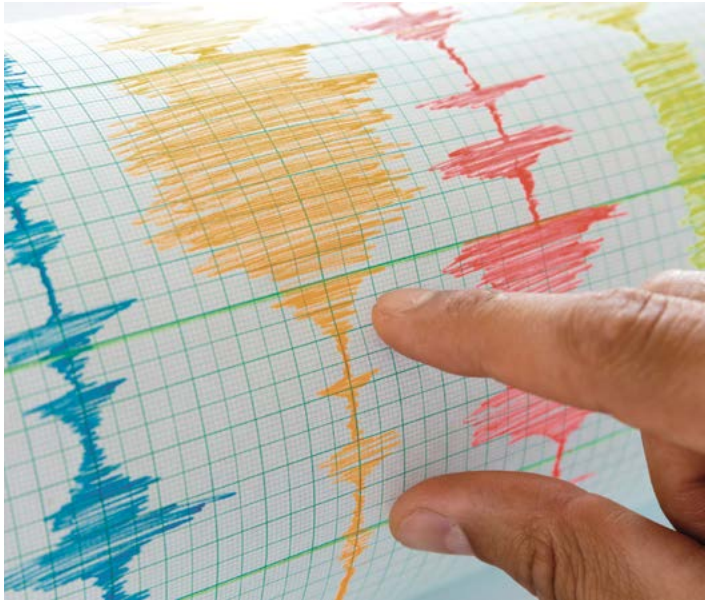
For life sciences contractors, natural disaster and supply chain risks are hardly new. According to the **2017 BDO Life Sciences RiskFactor Report**, 81 percent of the top 100 companies on the NASDAQ Biotechnology Index, not necessarily contractors, cited natural disasters as a risk in their most recent shareholder filings. Almost all (97 percent) mentioned supply chain issues, including product availability and compliance with Good Manufacturing Practices. Both risks have been tracked every year of the report's five-year history.

But Hurricanes Irma and Maria should serve as a stark reminder on the importance of disaster preparedness and supply chain balance. Many factories selected sites in Puerto Rico to take advantage of significant tax benefits, but those benefits of a reduced tax burden will no longer outweigh the supply chain risk associated with production that's concentrated to a single area. Looking ahead, pharmaceutical and device manufacturers—even those that haven't been directly impacted by the disruptions in Puerto Rico—would be wise to reevaluate supply chain risk.

Start with a broad risk assessment. This should begin at the top level of the organization, with an analysis of the risk related to natural disasters throughout the drug and device manufacturing process, including analysis of supply chain, regulatory, and reputation risks to which the company may be exposed. As natural disaster events persist, manufacturers should consider prioritizing these risk assessments. They can help them start to address short- and long-term threats, and create and implement manageable changes and solutions within both their supply chains and their production processes.

Pharmaceutical and medical device manufacturers can also take proactive steps to make plants more secure. Infrastructure investments for hurricane and fire-proofing or building remote storage, away from natural disaster-prone regions, will more than pay for themselves if and when catastrophe strikes.

Liability, property, and equipment insurance can also help to protect against these events. Pharmaceutical and medical device manufacturers make large investments in specialized equipment and warehousing space. Whether it's a small flood or a Category



Read more ▶

CONTINUED FROM PAGE 9

NATURAL DISASTER

5 hurricane, property and equipment insurance can minimize the impact to operations.

Pharma and device manufacturers should also ensure they are diversifying their suppliers and, perhaps most importantly, their production locations. This can help more adequately develop a supply chain able to withstand extreme weather. For investors in the space, conducting regular due diligence on supply chain risk is recommended.

The first several weeks following a big storm, businesses that are properly covered by insurance are likely beginning to check off steps on their emergency preparedness checklist. Those that don't have developed contingency plans, or are noticing gaps in their path forward, should consider incorporating the below next steps for coping with disaster and picking up the pieces.

1. **Communicate with employees and external stakeholders.** Following the activation of an emergency preparedness program, it is critical to communicate with employees and business partners about their well-being, as everyone will be dealing with potentially significant, or even devastating, personal and professional issues.
2. **Review your insurance policy.** Even if a business does not suffer physical damage, it may have coverage for business interruption losses. For example, if a business's customers or suppliers have been flooded and cannot receive the business's goods or services, the insurance policy may include what is referred to as "Contingent Time Element Coverage." Non-physical damage coverage for business interruption losses can also include lack of access to facilities (e.g., road closures) and loss of utilities, among others.
3. **Maintain contemporaneous documentation.** To say that the hours and days after a disaster are hectic is an understatement. This is a trying time for businesses as they try to rebuild and recover. However, keeping careful records even during this time of disruption is critical. Preserving email traffic around current market conditions and cancellations of sales or impacted suppliers/customers is critical to a business interruption claim.
4. **Get the right team on your side.** A major property claim can take several months to resolve, and the complexity of the issues that may arise requires external experts to look out for a business's interests while management focuses on what is important—rebuilding and recovering.
5. **Establish milestones for claim recovery.** Following a major catastrophe, resources are often stretched thin. It is important to create milestones and hold all members—from the adjusting team to internal stakeholders—accountable for achieving those goals.

*A version of this article also appeared in **The Pharma Letter**.*

Steven Shill, CPA, is an assurance partner and the national co-leader of the The BDO Center for Healthcare Excellence & Innovation. He can be reached at sshill@bdo.com.

Patrick Pilch, CPA, MBA, is a national co-leader of The BDO Center for Healthcare Excellence & Innovation. He can be reached at ppilch@bdo.com.

David Friend, MD, MBA, is chief transformation officer and managing director in The BDO Center for Healthcare Excellence & Innovation. He can be reached at dfriend@bdo.com.

Clark Schweers leads BDO's Forensic Insurance & Recovery Practice. He can be reached at cschweers@bdo.com.

DID YOU KNOW...

According to a **Professional Services Counsel survey**, 72 percent of CIO's of federal agencies say a majority of applications in their systems are out of date.

Washington Technology's Contractor Confidence Index has fallen more than 10 points since January to stand at 102.2 for the third quarter, indicating a decline in optimism among government contractors.

The $700 billion bipartisan National Defense Authorization Bill would reorganize the Department of Defense and raise defense spending, **Government Executive** reported.

A new **Government Business Council** survey reports that 60 percent of federal officials rate security as their top concern for Internet of Things (IoT) devices.

Read more ▶

SIGNIFICANT ACCOUNTING & REPORTING UPDATES

The FASB recently issued ***ASU 2017-11 (Part I) Accounting for Certain Financial Instruments with Down Round Features, (Part II) Replacement of the Indefinite Deferral for Mandatorily Redeemable Financial Instruments of Certain Nonpublic Entities and Certain Mandatorily Redeemable Noncontrolling Interests with a Scope Exception*** to simplify the accounting for certain financial instruments with down round features. This new standard will reduce income statement volatility for many companies that issue warrants and convertible instruments containing such features. It is available **here**, and becomes effective for public companies in 2019 and all other entities in 2020.

The FASB recently issued ***ASU 2017-12 Targeted Improvements to Accounting for Hedging Activities*** to improve its hedge accounting guidance. This new standard simplifies and expands the eligible hedging strategies for financial and nonfinancial risks. It also enhances the transparency of how hedging results are presented and disclosed. Further, the new standard provides partial relief on the timing of certain aspects of hedge documentation and eliminates the requirement to recognize hedge ineffectiveness separately in earnings. The ASU is available **here**, and becomes effective for public companies in 2019 and all other entities in 2020. Early adoption is permitted.

MARK YOUR CALENDAR...

DECEMBER

Dec. 19
ISS Cost Estimating Techniques*
Online Webinar

JANUARY

Jan. 25-26
FAR Workshop
NeoSystems Corp.
McLean, VA

** indicates BDO is hosting or attending this event*

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

People who know Government Contracting, know BDO.