WIPFLi LLP
CPAs and Consultants

Solutions for 6 Business Issues Causing You to Lose Sleep

The world is changing at a rapid pace. Each day, new challenges present themselves, keeping executives and business owners awake at night.

To help put your worries to rest, here are solutions to six current business issues.

1. New Revenue Recognition Standards

In what has been described as one of the largest changes to GAAP in over a generation, the Financial Accounting Standards Board (FASB) and the International Accounting Standards Board (IASB) issued new revenue recognition rules to bring consistency across industries, enrich financial disclosure, and enhance comparability for those relying on financial statements.

However, for financial accounting professionals, the new, consolidated contract revenue recognition standards—set to replace over 200 specialized and/or industry-specific revenue recognition requirements under U.S. GAAP—will result in massive changes to systems, processes, and accounting practices.

Who Does This New Guidance Impact?

The new guidance affects any reporting organization that either enters into contracts with customers to transfer goods or services or enters into contracts for the transfer of nonfinancial assets like real estate. All types of organizations —public, private, and not-for-profit—will be affected by ASC 606. The guidance applies to all revenue-generating activities except those stemming from loans, leases, investments, derivatives, guarantees, or insurance contracts.

The standard is effective for periods beginning after December 15, 2017, for public entities, which include not-for-profit entities that have issued or are a conduit bond obligor for securities that are traded, listed, or quoted on an exchange or an over-the-counter market. The standard is effective for all other entities effective for periods beginning after December 15, 2018.

The New Five-Step Model of Revenue Recognition

1. **CONTRACT: Identify the Contract With the Customer.** The standard defines contract very broadly. Generally, all transactions with a customer are covered, with just a few exceptions. Having said this, ASC 606 requires that customer contracts be enforceable. Assessing whether a contract is enforceable will require evaluation of five separate conditions set out in ASC 606. In a number of cases, the analysis may require a legal review.

2. **OBLIGATIONS: Identify the Performance Obligations in the Contract.** This step requires companies to determine the "accounting units" for a particular customer contract. Identifying "distinct" goods or services involves assessing whether an item is capable of being separate, as well as whether the item is viewed by the customer as being distinct within the context of the contract taken as a whole.

3. **PRICE: Determine the Transaction Price.** The transaction price is the amount of consideration to which an entity expects to be entitled. Estimating the transaction price can be challenging when the contract has elements of variable consideration, like bonuses.

4. **ALLOCATION: Allocate the Transaction Price to Separate Performance Obligations.** The transaction price is allocated to the separate performance obligations in a contract based on the relative standalone selling prices of the goods or services promised. This allocation is made at contract inception and not adjusted based on subsequent changes in the standalone selling prices of those goods or services.

5. **RECOGNITION: Recognize Revenue as Each Performance Obligation Is Satisfied.** An entity will recognize revenue when (or over time as) a good or service is transferred to the customer and the customer obtains control of that good or service.

Steps You Can Take

- ❑ **Build a Team and an Action Plan:** Planning for the transition to the new standard requires a discussion among functional groups who will be affected by the change, including finance, sales, IT, legal, and others. It is recommended to form a cross-functional task force to implement the new revenue recognition standard.
- ❑ **Educate:** Review the final standard and implementation guidance (ASC 606) to understand the complexities and pitfalls that implementation could pose for your organization. Consider bringing in specialists to provide training and help expedite the learning curve.
- ❑ **Evaluate Impact:** Identify the changes from current GAAP to the new revenue recognition standard and evaluate the potential effects on the accounting for existing revenue streams and the results of the company's financial performance. In addition, consider how the standard will impact operational and performance metrics, company contracts, compensation plans, accounting policies, internal controls, and tax matters, and communicate the effects to stakeholders.
- ❑ **Determine Adoption Method:** Determine how you will adopt the new revenue recognition standard and how to track the accounting differences for periods that require restatement.
    - o **Full Retrospective Method:** The full retrospective method requires companies to recast prior-period financial statements as if the guidance had always existed.
    - o **Modified Retrospective Method:** The modified retrospective method provides companies with some relief, since prior-year financial statements will not need to be recast. However, disclosure of what the financials would have looked like under existing GAAP is required in the year of adoption.

  The potential effects of ASC 606, and the method of adoption, must be disclosed in annual and interim reports.
- ❑ **Analyze and Assess:** Learn how the new standard will affect your current and/or ongoing business processes, tax compliance, commission arrangements, and internal controls.

  At this stage, an entity will need to consider whether its IT systems, data models, and related enterprise resource planning (ERP) software are able to capture, track, and report information in accordance with the needs of the new standard.
- ❑ **Update Applications and Processes:** If your systems and processes are not designed to handle the needs of the upcoming standard, it is necessary to find a solution that will be able to not only handle the new standard, but simplify your transition. As mentioned above, the new standard affects multiple functional areas.

Revenue Recognition
Need to learn more?
The clock is ticking to prepare your organization for the changes that will hit it in 2018 or 2019. The earlier you implement a plan, the easier it will be to transition.

In Chicago, contact Brad Werner to learn more about the skills and advice you need to remain compliant with this and other standards, as well as to save time and money through automation, process improvement, and advisory services.

2. Cybersecurity: Are You Incident-Response Ready?

When it comes to tornadoes, hurricanes, or other natural disasters, most organizations have a practical response plan, one that's practiced regularly and updated as needed. But when it comes to a cyber-attack, a missing or stolen laptop, or a curious vendor who helps himself to proprietary data, does your organization have a swift, practiced, and updated response plan?

Having a formal incident response and management plan in place and ready before you need it is crucial to information security. Here are some vital elements to consider for ensuring your plan covers all the fundamentals:

- **Define incidents.** Workers can't always identify an incident unless it's clearly defined. Some incidents are obvious ("My computer has a virus!"), but others are not as obvious ("That person is accessing PII, so they must have the proper clearance, right?"). As you develop your plan, broadly define what incidents are, but also spell out the many scenarios that qualify as incidents. Give your workers a clear picture of what an incident might look like.

  At the same time, be sure your organization recognizes the difference between a security incident and a data breach. A data breach is a serious incident whereby confidential information has in some way been compromised. A security incident is usually any other event that results in the inadvertent access or compromise of systems and/or information not classified as proprietary, a hacking attempt, malicious software, an attempted breach of the network perimeter, etc.

- **Establish reporting guidelines.** Once workers know how to recognize security incidents, they need to understand how to report them. Make reporting easy. It can be as simple as completing an online form or calling a 24/7 hotline. In addition, be sure to educate staff about the importance of reporting the incident in a timely manner.

- **Determine responses based on the type and impact of incidents.** The many types of security incidents and breaches differ and vary in their degree of severity. Organizations should recognize the unique differences and respond accordingly. For example, responding to a virus or cyber-attack requires a much different response than would be required for a lost laptop. Those differences will also determine which key members of an incident response team—from security and IT operations to HR and PR to legal—should be involved in responding to which events.

- **Consider your containment efforts.** Every plan must outline how and what will be done to limit exposure. Cyber-attacks require an immediate response and potential shutdown of services to limit the exposure or damage to other internal resources, whereas experiencing an insider or vendor stealing or inappropriately viewing data may require disciplinary action or termination. Timely reporting and early response cannot be overstressed.

- **Include remediation, also called recovery.** Your plan should include measures that address the most immediate aftermath needs (for instance, cleaning up computers post-virus), but also include a review or risk analysis of the circumstances leading up to the incident to determine what steps or improvements are needed to prevent a similar incident/breach in the future.

Subscribe to the WipfliSecurity Insider email to connect with Wipfli's security experts, get up-to-date guidance on the latest threats and fixes, new ideas for improving your security, and tips to help navigate compliance.

- **Remember reporting.** Here again, the type of incident will determine the degree of reporting; there are specific and regulatory-mandated requirements for reporting the most serious of incidents, a data breach. They include notifying state and federal officials, regulators, employees, customers, and even the public.

In addition to establishing a plan, here are some additional activities you should consider for your business to promote awareness:

- **Conduct Employee Cybersecurity Training.** There are helpful and free tools to assist at www.StaySafeOnline.org.
- **Test Emergency Communication.** Conduct an all-employee notification drill to test how quickly emergency messages can be distributed and verify that the contact information is correct.
- **Clean Desk Check.** Ensure all confidential information is secured by doing a walk-through of your office and provide positive reinforcement for employees who keep the workplace secure.

- **Phish your Employees.** Conduct an email phishing campaign to see how many employees are following policies and best practices for online communication.
- **Ransomware Exercise.** Facilitate a drill to simulate how to respond to a ransomware incident.
- **Backup and Recovery.** Make sure that your data is successfully backed up and verify that it can be restored by testing.

Learn more about Wipfli's cybersecurity services at wipfli.com/cybersecurity.

Need to learn more about our Cybersecurity services?

In Chicago, contact Matt Janoski for assistance.

3. Change Management: Key to Implementation Success

Effective change management has a significant impact on the likelihood of meeting a project's objectives, keeping costs under budget and staying on schedule, according to the 2016 report, *Best Practices in Change Management*, by research group Prosci. The latest data indicate that a project is six times more likely to be successful when there's excellent change management.

People tend to think of change management as "good communication," but that's only the beginning. While good communication is important in spreading information about the change, it shouldn't be mistaken for the change process itself.

The Association of Change Management Professionals, an international organization, defines the practice as "a deliberate set of activities that facilitate and support the success of individual and organizational change and the realization of its intended business results."

In practice, these activities often begin with assessing an organization's culture and dynamics through interviews, focus groups, or surveys and gathering information on past change initiatives to see which tactics worked and which didn't. In this people-centered approach, a change management strategist suggests the most effective tactics to guide change, weaving these activities with more traditional project management

activities. These tactics include explaining what's going to be different for each type of employee or group, including personnel in the process, and taking time to listen to and understand their concerns. All of these ultimately lead to people understanding the change and embracing it.

Major Obstacles and Success Factors

Here are five major obstacles organizations encounter when introducing significant change:

1. Lack of effective sponsorship in change management
2. Employee resistance
3. Insufficient resources for change management
4. Failure to integrate change and project management
5. Resistance from middle management

According to the Prosci report, the top five contributors to a successful project, such as a technology initiative, are:

1. Executive sponsors in active, visible roles
2. Change management structure in place
3. Resources dedicated for change management
4. Integration and engagement with project management
5. Employee engagement and participation

Maximizing Your Organization's Change Capacity

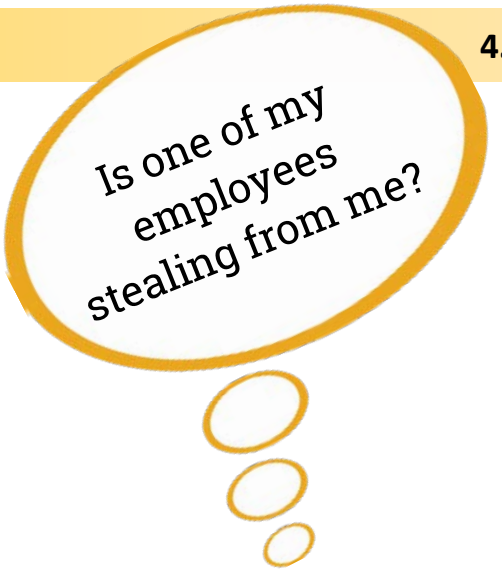
At the end of the day, it's important to understand that people have only so much capacity for change at any given time. Major initiatives don't unfold in a vacuum. Different departments and functions in your organization may already be confronting challenging transitions in other areas.

Want to make your technology initiatives more successful?

In Chicago, contact Jeff Wulf.

The role of change management, in a sense, is to assess and address these differences and to avoid overwhelming individuals while maximizing the organization's change capacity. Adopting this approach helps a company get the most value from its investments, while also keeping personnel engaged and motivated.

4. Occupational Fraud



Also referred to as workplace fraud or simply asset theft, occupational fraud is a daily risk and an expensive problem. The Association of Certified Fraud Examiners (ACFE) estimates that the typical organization loses 5% of revenues annually as a result of fraud. In 2016, total losses caused by the cases studied exceeded $6.3 billion, with an average loss per case of $2.7 million.

Given the enormity of the risk and costs and the prevalence of its occurrence, how fraud savvy do you believe you are? Could you identify fraud by way of suspicious behavior?

Identifying Red Flags

To reduce or avoid losses, organizations should learn to recognize a few warning signs. These red flags can be categorized into situational, opportunity, and characteristic variables or influences that can potentially result in fraud.

Situational red flags include employees with high personal debts or losses, those living beyond their means, and individuals with gambling, alcohol, or drug abuse problems. Such situations can present a strong motivation to steal. Indeed, a great many fraud cases are committed in order to meet personal financial obligations, particularly ones that have spiraled out of control.

Opportunity presents another temptation. This is the most controllable area for a company. Often, small businesses invest far too much trust in key individuals without instituting the necessary balance of controls. Opportunity red flags can include dominant employees who are intimately familiar with operations and those with close supplier or vendor associations.

Lastly, *character traits* can also serve as red flags. Studies have shown that employees who engage in workplace abuse such as excessive absenteeism, pilfering, and goldbricking are at higher risk for committing fraud.

All Kinds of People

Clearly fraudsters have many faces and backgrounds, and there's no such thing as a typical perpetrator. Despite the wide variety of traits and behaviors, there are genuine patterns and authentic trends that can help organizations become more aware of and responsive to fraud.

Consider these profile facts uncovered by the recent ACFE report:

- Fraudsters are nearly twice as likely to be male than female. In addition, losses attributed to males were higher than losses caused by females.
- Over half of perpetrators had a college degree.
- Seventy-seven percent of all occupational frauds originated in one of seven organizational departments: accounting, operations, sales, executive/upper management, customer service, purchasing, and finance.
- The majority of frauds are committed by staff at the employee or managerial level. However, the higher the fraudster's position of authority, the greater the losses. ACFE surmises that's because executives have greater access to assets and a better ability to evade or override antifraud controls.
- Fifty-two percent of fraudsters are between 31 and 45 years old, but older fraudsters tended to cause greater losses.
- Only 7% of perpetrators committed fraud during their first year on the job. In contrast, 53% had been with their organizations for more than five years. In addition, the longer a fraudster had worked for a company, the more harm (losses) he or she was likely to cause.

To sum up, your biggest risk is from employees who are longer tenured, more experienced, better educated, and more trusted. Just the kinds of employees you want and value! It's easy to see why spotting and preventing fraud is such a difficult and ongoing challenge.

All Kinds of Schemes

Occupational fraud is typically classified into three categories: asset misappropriation (embezzlement, theft of cash or other assets, false expense reports, forgery, check tampering, billing schemes), corruption (conflict of interest, bribery, extortion), and financial statement fraud (fictitious revenues, inflating assets, concealing or underreporting expenses or liabilities).

Among the three categories, asset misappropriation is most prevalent, representing 83% of fraud cases reported in 2016. The median loss for victim organizations in these cases was $125,000. In contrast, fewer than 10% of cases involved financial statement fraud, but such cases had the greatest financial impact, with a median loss of $975,000.

There's no doubt that occupational fraud schemes are extremely costly. Overall, the median loss reported in the most recent ACFE study was $150,000. Just under one-quarter involved losses of $1 million or more.

Since fraud schemes frequently continue for years before they are detected, such losses have a way of adding up. The median duration of the frauds committed was 18 months, with nearly a third of them lasting two years before they were detected.

Some common examples of fraud schemes across various departments include:

Travel and Entertainment

- Double dipping. Submitting the same expense for reimbursement more than one time.
- Unauthorized expenses. Obtaining reimbursement for expenses not allowed under company policy.
- Bait and switch. Getting preapproval for one type of expense but then purchasing a different and less expensive item and receiving the higher, preauthorized amount.

Purchasing

- Conflicts of interest. The person purchasing items has a conflict of interest in which judgment may be compromised, such as an ownership interest in the vendor or being related to a vendor owner or a vendor's employees.
- Collusion. Instances such as bid rigging, kickbacks, or purchasing inferior products, in which a person inside the organization works in concert with someone outside the organization and steers business to a particular vendor. (The larger the group of colluders involved in a fraud scheme, the greater the damage.)
- Credit/P-cards.

Payroll

- Ghost employees. Individuals who don't really exist get hired and paid, or terminated employees continue to get paid (usually the pay goes to the supervisor responsible for hiring and approving pay).
- Hours/pay schemes. Employees, with or without the assistance of supervisors, submit time not worked or time coded at higher-paid duties than were actually worked.

Accounts Payable

- Fictitious vendor. Creating and processing payments to a vendor that doesn't exist for goods or services never received.
- Check tampering. Includes check forgery, altering payees, or forging the endorsement of checks payable to a legitimate vendor.

Start to Outsmart Fraud with Smart Internal Controls

Clearly, having a fraud prevention program and proper internal controls is vital, as the ACFE report bears out. When fraud was uncovered through active detection methods such as surveillance and monitoring or account reconciliation, the median loss and

median duration of the schemes were lower than when the schemes were detected through passive methods such as notification by police or accidental discovery.

And yet smaller organizations continue to have significantly lower implementation rates of antifraud controls than large organizations. This gap in fraud prevention and detection leaves small organizations (those with under 100 employees) extremely susceptible to fraud that can cause devastating damage to their limited resources.

Fraud risk management requires several fundamental factors, the first of which is having proper internal controls. Among them are:

- Robust internal control environments
- Conducting risk assessments
- Instituting control activities like policies and procedures, segregation of duties, and surprise internal and external audits, for example
- Ensuring ongoing employee training
- Monitoring and acting with a response plan

These are just the building blocks for developing an effective antifraud strategy. Recognize the harsh reality that fighting fraud is difficult and time consuming but necessary. Get expert help with extra vigilance and targeted strategies whenever you need it.

Are you concerned about fraud in your organization?

In Chicago, contact David Friedman to discuss your fraud concerns.

5. Tax Issues

Tax return preparation is more than merely completing tax forms every year. With a wider perspective, the task of preparing a return evolves into a strategic opportunity to proactively seek additional tax planning opportunities. Below are a few of the current hot tax topics to consider:

- **Research and Development Tax Credits**
  Many businesses overlook a tax incentive for R&D activities at the state, federal, and global level. The tax law is complex and sometimes applies to varying aspects of a business not traditionally thought of as pure R&D activities.

  Normally, when companies think of R&D, the focus is on the development of new, cutting-edge products or design standards for an industry. While these highly technical activities generally qualify for the research credit, many of the day-to-day activities of companies may qualify as well such as improvements made to products or business operations.

  For income tax purposes, the definition of a qualified activity for the R&D Tax Credit (also referred to as the Research & Experimentation Credit or Research Credit) includes new or improved products, processes, techniques, formulas, patents, and software applications.

Proper understanding of the power of this tax credit could generate tax savings opportunities to lower tax liability and, therefore, increase cash flow available for other needs.

Learn more about the research and development tax credit and the benefits your business can gain…

Contact Chris Blaylock in Chicago

- **State and Local Tax Incentives**
  Many times there's an unanticipated tax benefit when businesses make a routine investment in people, processes, or capital expenditures. Don't miss out on qualifying for a tax incentive available from state and local government resulting in significant tax savings. Experienced tax specialists help identify events that trigger lucrative tax credits and incentives such as:

  - **People** - Hiring credits, training grants or incentives.
  - **Capital Expenditures** - Many states have development zones or programs that encourage companies to make significant capital investments in those states, areas or regions.
  - **Operations** - Most states "piggy back" off the federal research and development tax credit. They also have other programs to incentivize manufacturing, energy and sustainability plans, and provide exemptions from property taxes and other local taxes.

  Credit and incentive programs vary tremendously from state to state. In addition, many programs may be statutory while others are discretionary and require significant up front negotiations with state and local agencies. Partner with a proven team to help investigate the programs that align with your strategic goals and assist with negotiating a credits and incentives package.

- **State Tax Compliance**

As companies continue to expand their sales across the country, a growing company may not realize the required tax filings needed in the various states. Oftentimes, it may take a state a few years to catch up with a new taxpayer…but eventually they need to pay the piper.

The states have been becoming more aggressive as the desire and need to collect more revenue grows. As state technologies advance, locating noncompliant taxpayers becomes easier than ever before. If no tax returns are discovered a letter to the company is often sent inquiring whether they have "nexus" in their state for tax filing purposes. Additionally, states are able to match up their own state filings. For example, if a company is registered and remitting paying unemployment tax or withholding tax in a state, but no other tax filings, this would likely result in correspondence to the company to identify if the company has the needed connection or "nexus" for the state to impose its income tax filing requirement on that company. How about when a company for legal reasons decides to register with the Secretary of State to transact business in the state as a foreign corporation, but files no other tax returns in a state. Often times the letter will be sent asking the company to explain why they are registered with the Secretary of State to transact business, but not filing any tax returns.

States also find non-filers through audits of companies that are currently filing in the state. If your customer is going through a sales and use tax audit, the state may see an invoice with your company name on it, or if you are driving a company vehicle through the state, an auditor may see your logo and look up your filing record with the state. Likewise, if your company is involved with a trade association or business group—for example, a construction management association local branch, the state may see this and be prompted to investigate further.

Questions on State and Local Taxes?

Contact Jessica Macklin with all your State and Local Tax questions.

Read Seven Noteworthy Trends and Highlights in State and Local Tax for more information on this topic.

Once a state has a company's name, they are able to go to a company website. This website, while many times geared toward a customer's use, can be used as a road map for an auditor. Many times, a website boasts maintenance services that will be provided across the country and to every customer. In addition, the website may state customer testimonials with actual company information. To a customer this is appealing, to an auditor this is revealing a nexus creating activity which gives rise to a filing requirement in these states.

Some companies are required to meet certain criteria in order to hold a license for operating their specific business in a state. For example, one of the requirements to be a dealer of vehicles in a state may be to have a storefront with a sign indicating the location of the business. To meet this requirement, some companies will rent a small amount of space out of a local storefront in the state in which they want to operate. While this meets the requirement for the dealer license in the state, it also unwittingly created nexus for that company in the state since the company then has a "business location" in the state. There are many activities that make sense from a business perspective, but also have state tax filing ramifications.

To ensure compliance, it is highly recommended to have a nexus study performed to verify you have all of your necessary states covered from a tax filing perspective. Once a nexus study is conducted it should not be a one and done event. It should be done on an ongoing basis because companies can change over time, including product sales and market channels.

6. Information Integration

From manufacturing to private equity, businesses are engineered to deliver products and services to meet customers' needs. There are potential issues with every facet of how these products and services are delivered – from purchasing, manufacturing, logistics, and warehousing through employee and vendor management – which may be keeping business owners and managers up at night.

Enterprise Resource Planning (ERP) helps get work done and meet customers' needs, allowing businesses to focus on organizational goals.

Here are some best practices to ensure a successful ERP implementation:

- **Identify an all-in-one business solution that's easily expandable.** Using a system that doesn't already have the modules you might need—CRM or e-commerce, for example—will ultimately require adding disparate systems and essentially put you back where you started. By contrast, the right solution will already have all the components needed: NetSuite® or Microsoft Dynamics 365, for example. Both solutions allow you to add users, modules, and processes to further expand the platform as you grow and your needs evolve.
- **Identify an end-to-end standard up front.** The goal is to consider all the features needed and "bake in" all those possibilities up front. Then you can weigh each business against the overall solution and adapt it for each unit by simply deleting what's not needed, versus customizing and adding from scratch each time an organization is rolled up.

- **Adopt standard, cloud-based platforms for greater automation and reduced IT overhead.** For many, the strategy of the future is to keep IT overhead light and reduce the number of FTEs required. Successful firms have identified the value of relying on consultants in the short term, fully knowing that the new cloud-based, scalable solutions will allow them to run even leaner in IT going forward.

- **Manage Expectations and Change.** It's critical that a company makes an effort to clearly and frequently communicate with its people throughout the process, particularly at the outset. Employees will be concerned about how the ERP will affect them (Will it mean changes to their job descriptions? Will their workload expand? Will they have to learn new software?), the reasons for the change, and how that change will take place.

  Perhaps the biggest employee concern we encounter when implementing an ERP is related to productivity. Many companies hold their teams responsible for a specific level of productivity, so when those employees are told that an ERP system comes with a sometimes steep learning curve, they may fear they'll struggle to achieve their goals.

  The more your employees know about the purpose and benefits of an ERP and what's expected of them during the project and the use of the system in the future, the more likely they'll be to embrace it.

- **Training.** People often push back when told about the new ERP software, but it's not because they don't believe it has long-term value. They're usually reluctant because they fear they won't know how to use it. A detailed training schedule and dedicated time to practice will help them feel comfortable with the tools and their ability to properly use them.

Perhaps the best way to ensure a smooth, stress-free implementation is to work with professionals who not only know the ins and outs of ERPs, but also know your business.

Learn how our insights and the right ERP solution can help you build a profitable, scalable business solution.

If you're considering an ERP system, contact Jeff Wulf.

About Wipfli

With over 1,900 associates, 45 offices in the United States and two offices in India, Wipfli ranks among the top 20 accounting and business consulting firms in the nation. Wipfli is also a member of Allinial Global, an accounting firm association of legally independent accounting and consulting firms with offices in North America and throughout the world through international members and partnerships.

We enjoy a solid reputation as industry specialists and as a trusted business advisor to more than 60,000 clients including: manufacturing companies, construction companies, contractors and developers, real estate companies, health care organizations, financial institutions, insurance companies, nonprofit organizations, units of government, dealerships, and individuals.

The firm serves businesses of various sizes, from large public and private companies, to closely held family-owned businesses. Whether we're helping clients streamline processes, improve performance, leverage the right technology, or increase financial success, we offer innovative, effective, and personalized services to help clients overcome their business challenges today and plan for tomorrow.