Deloitte.

2015 Energy Compliance Survey Report

Energy industry leaders share their latest thoughts on regulatory compliance in the US

Introduction

It is no secret that energy companies continue to face evolving regulatory challenges, which requires continuous monitoring and assessment of risk, resource allocation and adaptation of controls. As a result, entities are seeking new and creative ways to improve the efficiency and effectiveness of their compliance programs in order to keep pace with the oversight and enforcement activities of regulatory authorities such as the Commodity Futures Trading Commission (CFTC), North American Electric Reliability Corporation (NERC), and Federal Energy Regulatory Commission (FERC). In this constantly shifting environment, Deloitte's annual compliance survey is designed to help energy companies accomplish these goals, sharpen their approach to compliance, and provide new insight into how the industry is designing and implementing compliance programs.

This report highlights our key findings and has been grouped into four categories that are generally of the most interest within the energy industry – Enterprise Compliance, NERC, FERC, and CFTC – so you can focus on the regulatory areas that matter most for your business.

Fifty-one companies participated in this year's survey, including major oil companies, integrated utility companies, independent power producers, and independent system operators. Respondents included Chief Compliance Officers, Senior Compliance Directors/Managers and Associate/ General Counsels. The commercial footprint of the participating companies spanned more than 40 states and half of the Canadian provinces.

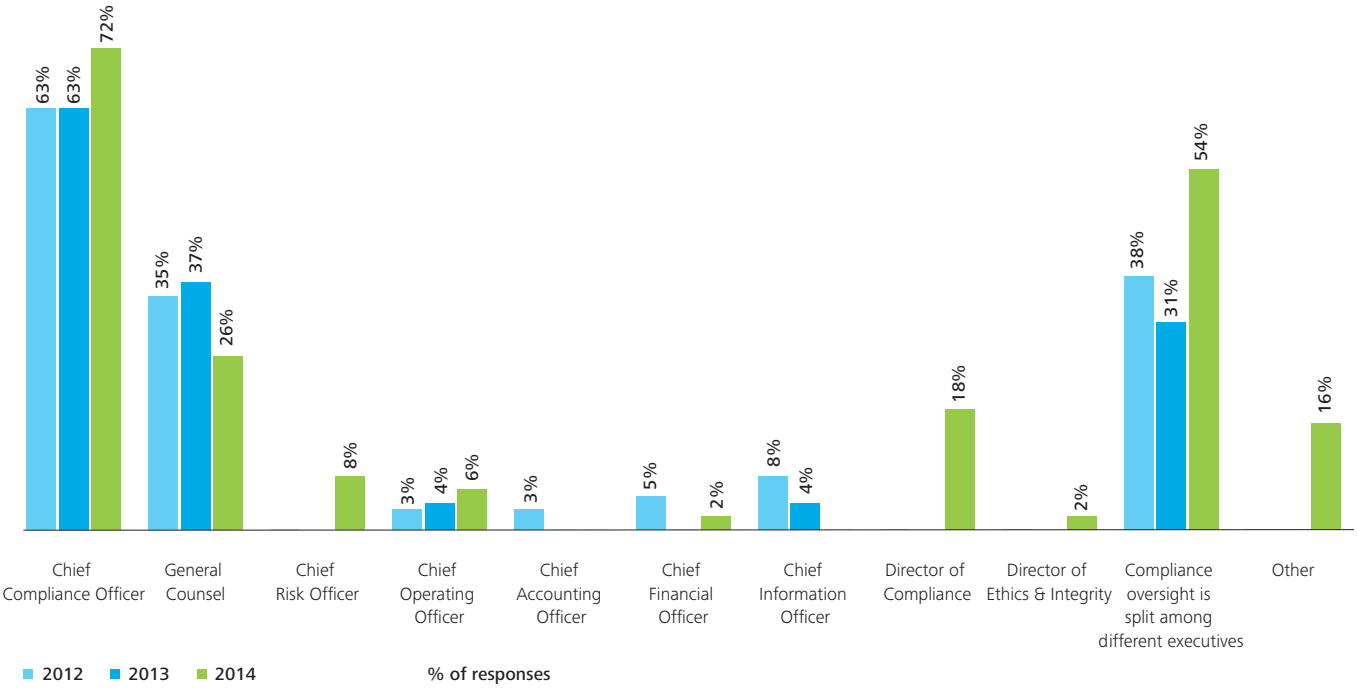
Enterprise Compliance

Centralizing versus decentralizing compliance management and oversight

One of the top challenges companies face when applying an enterprise compliance lens is to determine the right structure for governing their programs – i.e., centralized versus decentralized versus a hybrid approach – and how best to allocate resources across the organization to manage the extensive compliance obligations at hand. In the energy industry, it is common to find diverse teams of business and technical specialists, enterprise risk management specialists, risk and control professionals, compliance officers and directors, internal auditors, and others working together to help their companies manage risks, including compliance risks. An effective approach to governance requires collaboration across multiple functions and business units, strong leadership and clearly defined accountabilities across all levels, combined with a robust risk-based approach for efficiently allocating resources.

This year's survey results show a substantial increase in the number of energy companies that centralize multiple components of their compliance program under a single Chief Compliance Officer, from 63 percent in 2012 and 2013 to 72 percent in 2014.

Figure 1: Who within the company has oversight responsibility for the enterprise compliance program? (Select all that apply)

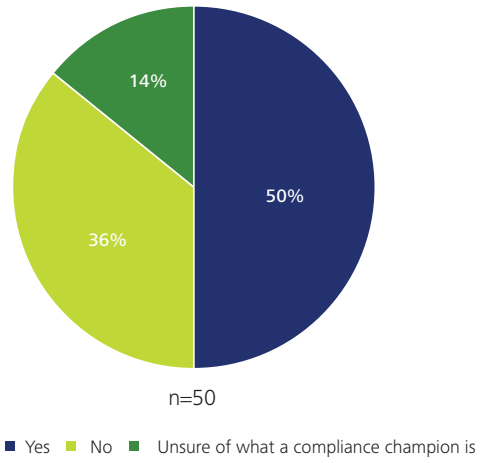


Note that this shift toward centralization of compliance activities under a Chief Compliance Officer does not absolve other executives of their responsibilities for overseeing regulatory compliance. In fact, the number of companies that split compliance oversight among different executives is also up markedly, from 31 percent in 2013 to 54 percent in 2014. What's more, three-quarters of the surveyed organizations have a compliance committee in place, 84 percent of which are comprised of executive officers. Taken together, these trends suggest energy companies are becoming increasingly focused on the management of and accountability for regulatory compliance – creating centralized roles to provide overall management and monitoring of compliance activities at the enterprise level, while at the same time holding executives within the business increasingly accountable for day-to-day compliance oversight.

Compliance champions

A common challenge associated with managing an enterprise compliance function, which often operates with scarce resources, is the ability to maintain awareness and visibility into the assorted compliance activities occurring across all levels and all areas of the organization - particularly on the front lines or deep within the business. Compliance champions are an increasingly popular solution to address this challenge – assigning selected individuals within the business units to provide informal feedback to the enterprise compliance function and help it stay informed. This is especially important for areas of compliance oversight that remain disaggregated in the business units – areas where the enterprise compliance function does not have full oversight responsibility, but is still expected to maintain visibility and awareness. According to our survey, 50 percent of energy companies have designated compliance champions within their organizations.

Figure 2: Does your organization have personnel akin to "compliance champions" embedded within the business units to serve as a primary point of contact for the enterprise compliance function?



There is no secret formula to determine the number of champions required to make this model a success. The answer varies widely based on factors unique to each organization, including the size of the organization, the number of business units, the types and extent of regulation applicable to the organization, the business units' expectations for these individuals, and the size and structure of the compliance function.

Using risk assessments to drive compliance focus, budget, and staffing

The vast majority of organizations we surveyed now regularly conduct enterprise-level assessments of compliance risk, most of them annually (71 percent - up from 60 percent in 2013) (figure 3). Yet not many entities are using their findings to make better decisions. According to the survey, only 37 percent of respondents use the results of their risk assessments to help allocate staff based on relative risk (figure 4). This suggests that energy companies might be missing out on time and cost efficiences because allocations are not informed by or focused on an understanding of the relative risk for the particular area or activity. It also begs the question of why the assessments are being performed in the first place – whether the output is adding value or if it is viewed as more of a check-the-box exercise. With compliance resources typically scarce, it's more important than ever to focus where it really counts – on the areas of highest risk to the organization.

Figure 3: How frequently does your company perform an enterprise level compliance risk assessment?

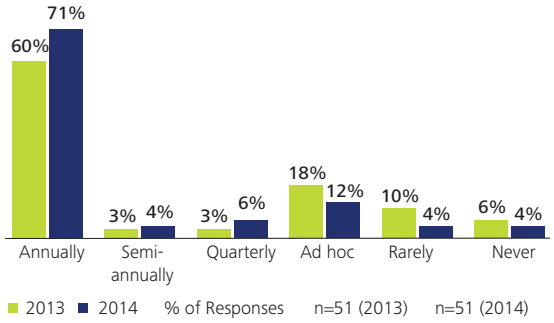
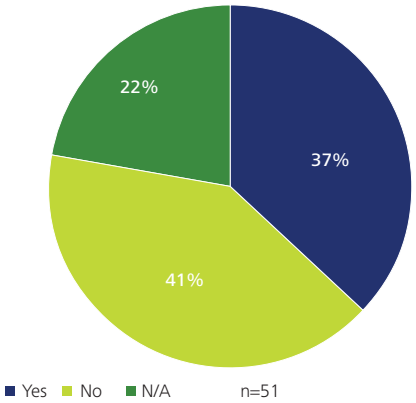


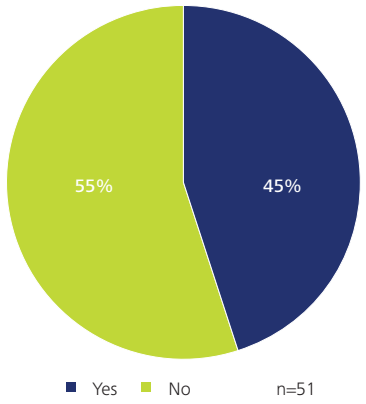
Figure 4: Do you use the results of the enterprise compliance risk assessment to facilitate staffing allocation decisions (e.g., shifting resources to high risk areas)?



Measuring effectiveness

The survey results show that more than half of the organizations (55 percent) don't have a method for measuring the effectiveness of their enterprise compliance program (figure 5). Many organizations tend to focus on doing what is required day-to-day to comply with regulations, but few are able or understand how to apply a wider and more strategic lens to understand whether their overall compliance efforts are as effective as they could be.

Figure 5: Do you have a method for measuring the effectiveness of your enterprise compliance program?



Similarly, most surveyed organizations don't have a way to quantify if they have effectively established a culture of compliance. Not only is this one of the keys to achieving compliance that lasts, but is also a specifically defined FERC and NERC internal control and mitigating factor which regulators consider in determining enforcement sanctions.

Forward-looking metrics

Compliance metrics have traditionally focused on past performance – with a particularly strong emphasis on compliance fines and near misses. However, our survey shows that a growing number of companies are using forward-looking metrics that seek to identify potential compliance problems before they occur. Some of the more popular leading indicators currently in use include:

- Tracking the results of controls testing versus expected performance.
- Conducting a risk assessment (and possible gap analysis) to identify trends.
- Tracking and analyzing events, projects, mitigation plan completion, and other data points to spot trends and opportunities.
- Analyzing issues and/or near misses logged over time to reveal trends and patterns.

These leading indicators are not yet in common use, as many companies are still determining which ones are most effective. However, the use of forward-looking metrics has significant potential to help companies reduce compliance risk by proactively managing issues.

Key takeaways

- **Challenge whether you are maximizing the value of your compliance risk assessments.** Are you doing them simply as a check-the-box exercise? Do they drill down into enough detail to effectively assess compliance risk across the organization? Are you using the results to inform staffing allocation decisions that can make the most of your scarce compliance resources?
- **Make the effort to measure compliance effectiveness.** Establishing common metrics and analytic methods for tracking performance and effectiveness today - and over time - can help a company's compliance function deliver lasting results. Energy industry benchmarks can help you determine how your compliance programs stack up against those of your peers, and how to drive greater compliance and efficiency.
- **Use leading indicators to proactively manage compliance risks.** With regulators increasingly expecting companies to monitor themselves, compliance organizations need to establish preventative measures that can help identify potential issues before they turn into problems.
- **Focus on high risk areas without losing sight of other risks.** As you shift your attention away from low and medium risk areas, think about how techniques such as compliance champions can be used to maintain a line of sight without requiring direct, day-to-day involvement.
- **Understand your regulator's view on the relationship between compliance and risk.** Both state and federal regulators are placing a more emphasized view on risk based approaches to compliance and budgeting.

NERC

NERC budgets and staffing are on the rise

Of the three regulatory areas covered in the survey (NERC, FERC and CFTC), NERC compliance tends to receive the most attention in terms of staffing and budget. Most of the companies surveyed (69 percent) have a separate and distinct budget for NERC compliance oversight activities, and nearly half report an annual NERC budget in the range of $1 million to $2.5 million. More than half of the surveyed companies (46 percent) increased their budgets over the preceding 12 months (figure 6), and 44 percent increased staffing (figure 7).

Figure 6: Has the company's budget for NERC compliance activities stayed at the same level, increased or declined over the past 12 months?

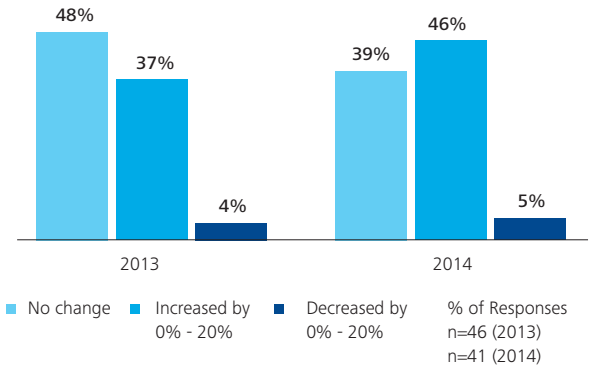
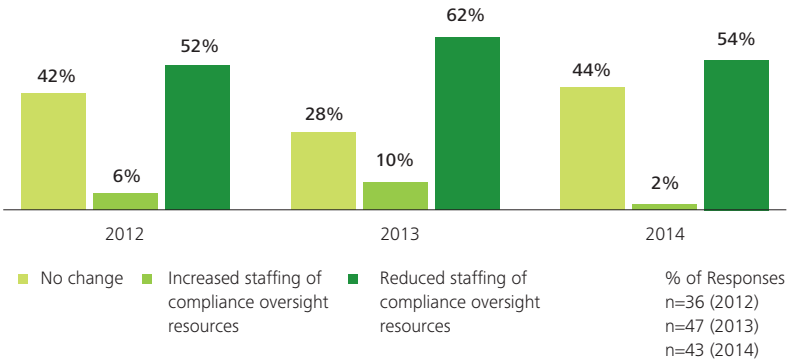


Figure 7: Has the company's staffing of NERC compliance resources stayed at the same level, increased or declined over the past 12 months?



These trends are not surprising given some of the major initiatives in the pipeline for NERC – namely, version 5 of the Critical Infrastructure Protection standards (CIP v5), as well as changes to the Compliance Monitoring and Enforcement Program driven by the Reliability Assurance Initiative (RAI).

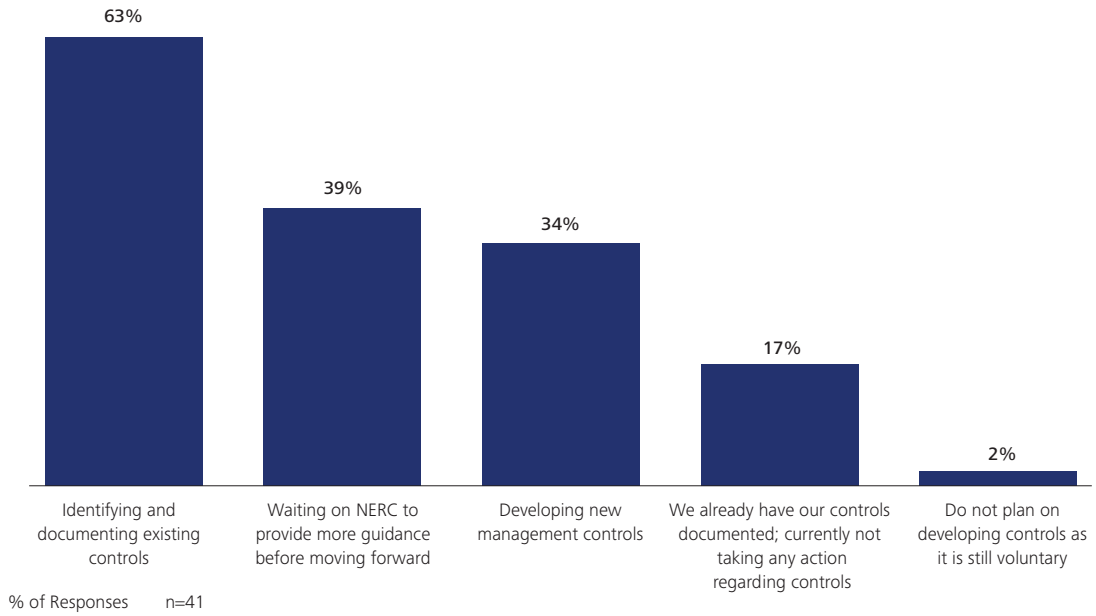
RAI is having less of a resource impact than expected

RAI (now formally known as risk-based compliance monitoring and enforcement) appears to be having less of a resource impact than initially expected, both in terms of dollars and headcount. At the time of our survey, 59 percent of respondents had spent less than $100K on preparing for RAI, and 52 percent expected to spend less than $250K total on implementation activities. When RAI's internal control concepts were first introduced, many energy companies viewed them as a potentially cumbersome set of new challenges. However, most entities seem to have slowed their plans for implementation to allow time to better understand how RAI will be applied and implemented by the regulators.

The most common actions energy companies are currently taking related to RAI are (1) tailoring their approach to assessing NERC specific-risks (59 percent), and (2) undertaking an exercise to identify and document existing management controls that are already in place (63 percent). A much smaller number (34 percent) are taking on the challenge of developing entirely new management controls.

Entities that are approaching RAI more strategically may be able to utilize the underlying risk-based concepts to inform or also better support risk assessment and management activities across other compliance areas.

Figure 8: What is your approach to addressing the internal control concepts proposed as part of RAI? (Select all that apply)



CIP v5 is having a major impact

At the other end of the spectrum, the move to CIP v5 – which represents the biggest change in the CIP standards since they were originally introduced - is having a major impact on the industry. Nearly half of the companies surveyed (48 percent) have already spent more than $500K preparing for CIP v5, with 30 percent having already spent over $1 million. In terms of anticipated total spend for preparation efforts, 56 percent expect to spend more than $2 million, with 28 percent expecting to spend more than $5 million. The highest impact challenges associated with CIP v5 implementation are: (1) an increase in the number of in-scope assets, (2) implementation of new systems, and (3) enforcement of the new requirements, along with the necessary cultural shift.

Rate the following challenges in terms of their impact on your CIP version 5 program implementation:

Figure 10: Talent supply and market availability of specific skill sets

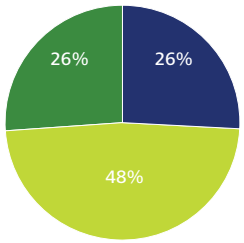


Figure 11: Increase in number of in-scope systems

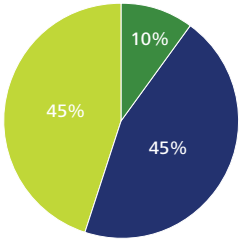


Figure 12: Talent management including background investigations, training, etc.

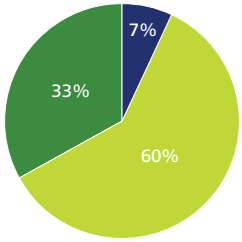


Figure 13: Cultural shift and enforcement of compliance requirements and business practices

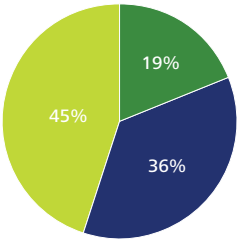
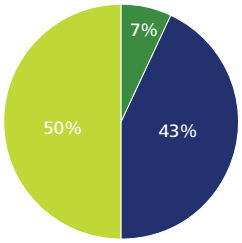


Figure 14: Implementation of new systems



High Medium Low n=42

Although companies must be in full compliance by April 1, 2016, for high -and medium-impact Bulk Electric System (BES) Cyber Systems, it appears that many still have multiple years' worth of work to do - with less than a year in which to accomplish it. This may create a significant resource strain as entities move closer to implementation. Frequent assessments of remaining activities against resource plans should be completed to mitigate the risk of a potential violation. On a positive note, 82 percent of companies say they consider their systems and infrastructure more secure as a result of the investments they have made in CIP compliance.

Key takeaways

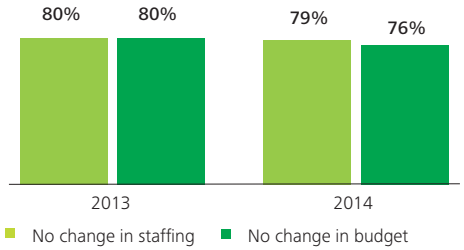
- **Take advantage of the investments being made in NERC compliance this year.** Since 2015 is a transition year - with major investments being made in NERC programs throughout the industry - this is an ideal time to pilot the risk-based concepts discussed in the enterprise section above. As you look ahead to the April 2016 milestone for CIP v5, challenge your existing approach to assessing NERC risks and explore how to best leverage the results of your risk assessments to allocate staff more efficiently and effectively.
- **Get ahead of the culture shift associated with CIP v5.** Overcoming resistance to change and establishing a culture of compliance will arguably be the biggest challenges associated with the move to CIP v5. Don't underestimate the on-the-job training and job shadowing that will be required to achieve and sustain compliance. Start now to provide foundational levels of training ("NERC 101") to field personnel who haven't had to comply with NERC in the past but have a higher probability of being in scope based on the new impact rating criteria.

FERC

Budgets and resources are flat

Although FERC's increasingly active approach to enforcement and fines has garnered significant attention, the underlying regulations and requirements have not changed much. As a result, most of the surveyed companies seem comfortable with their existing levels of effort and investment in this area. For the vast majority of companies (at least 76 percent), annual budgets and staffing for FERC compliance activities have essentially remained flat over the past several years (figure 15).

Figure 15: Has the company's staffing and budget for FERC compliance oversight resources and activities stayed at the same level, increased or declined over the past 12 months?



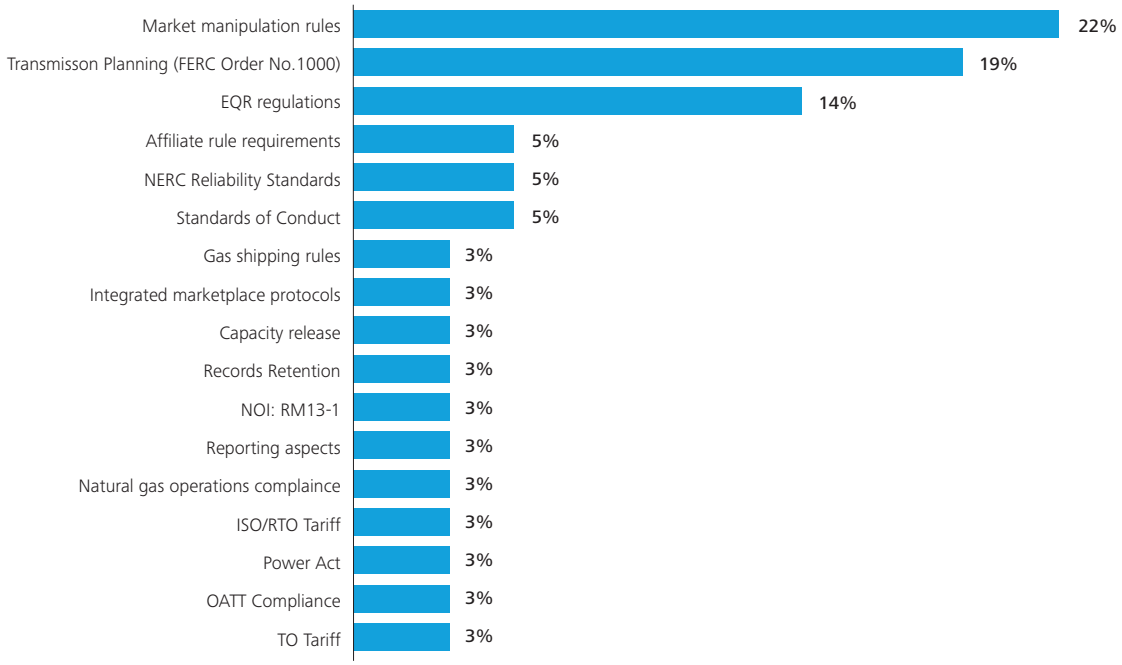
Although many companies rate FERC regulations as clear and understandable, more than half (56 percent) see significant room for improvement. Key issues cited by survey participants:

- Lack of a clear definition for key terms such as "market manipulation" with little or no legal precedent from the courts.
- Practical enforcement through independent market monitors that have no formal accountability structure.
- Difficulty applying FERC rules to diverse situations not specifically contemplated by FERC.
- Lack of a single, integrated source for all FERC information – such as rules and orders - on a particular topic.

Top challenges for FERC compliance

The top three most challenging FERC regulations to comply with, consistent with previous surveys, continue to be (1) market manipulation, (2) FERC Order 1000, and (3) electric quarterly reports (EQR) (figure 16).

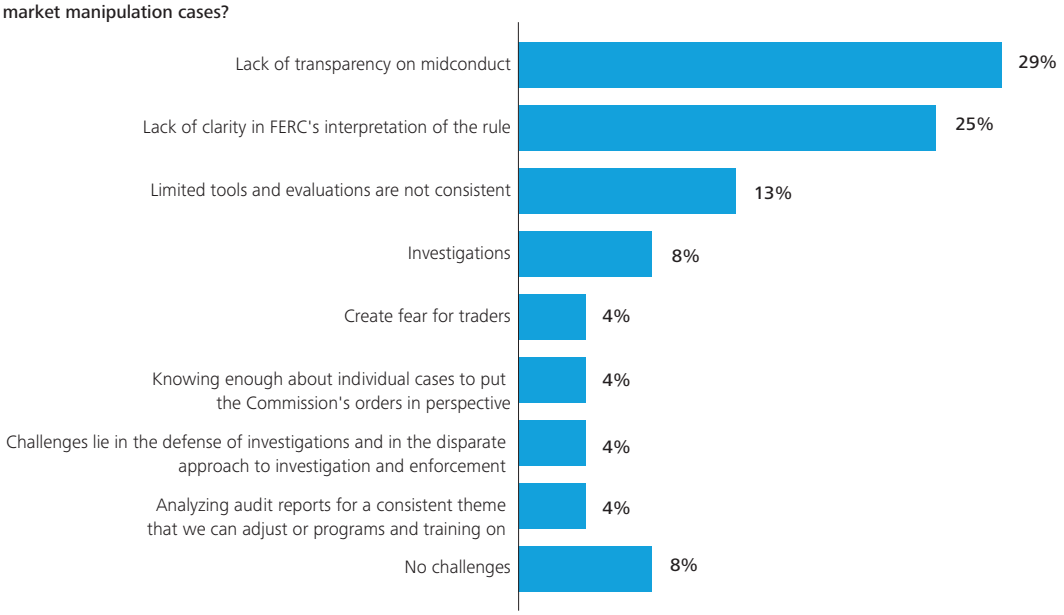
Figure 16: What FERC regulation (or anticipated regulation) is the most challenging to comply with?



Focusing on market manipulation

To address how FERC is handling market manipulation, many companies are making significant changes which include: allocating more resources to respond to FERC data requests, enhancing training and awareness programs, and improving internal process documentation. The biggest challenges appear to be lack of transparency about what constitutes misconduct, and lack of clarity about how FERC is interpreting the rules (figure 17).

Figure 17: What are the challenges you have with the manner by which FERC is approaching the investigation and enforcement of market manipulation cases?



Although the issue of market manipulation received significant attention and effort in 2014, many energy companies are still struggling to understand what constitutes illegal and inappropriate behavior. Despite hundreds of pages of guidance, considerable room for interpretation remains and many companies are still addressing potential risks on a case-by-case basis. Additionally, FERC continues to shift the tools and resources being used to identify violations so entities must remain vigilant in their understanding of what types of activities and data are informing these violations and whether the entity has controls that address these shifts.

The survey did reveal a number of common actions/controls within the industry. For example, the vast majority of companies (72 percent) are recording trader communications - particularly phone, email, and instant messages. Also, more than half (62 percent) have established monitoring/surveillance programs to periodically select and review samples of trader communications.

Key takeaways

- **Monitor spending on FERC compliance.** Since there aren't many new requirements in this area, spending on FERC compliance is becoming more targeted and most companies seem comfortable with their current capabilities and investment levels. One issue receiving increased attention and investment is surveillance to mitigate risks related to market manipulation and fraudulent commercial practices. However, unless your business is actively addressing such an issue, significant increases in FERC compliance spending and headcount could be a red flag to your leadership that is worth looking into.
- **Focus on the basics.** Better transaction monitoring can help organizations avoid problems without requiring a large investment of time and resources. Basic systems for monitoring and surveillance could enable rapid identification of risky transactions that might attract scrutiny from regulators. Another relatively easy improvement would be to reconcile internal hedge definitions to reflect guidance from both accounting and risk.

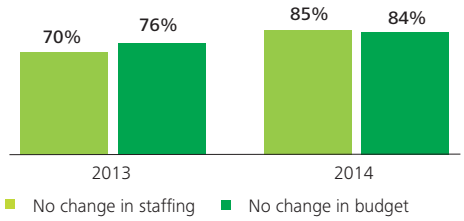
CFTC

The CFTC continues to expand its oversight of financial activities in the energy sector. Title VII of Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) made the CFTC responsible for providing greater transparency in the over-the-counter derivatives market, which includes using swap trades to hedge risk exposure in the energy markets. In 2014, the CFTC www.cftc.gov obtained a record $3.27 billion in monetary sanctions and filed 67 new enforcement actions. Also, it opened 240 new investigations.

Budget and resources

Despite the CFTC's heightened activity, annual budgets and staffing for CFTC compliance have remained flat over the past few years for more than 84 percent of the companies surveyed.

Figure 18: Has the company's staffing and budget for CFTC compliance oversight activities and resources stayed at the same level, increased or declined over the past 12 months?

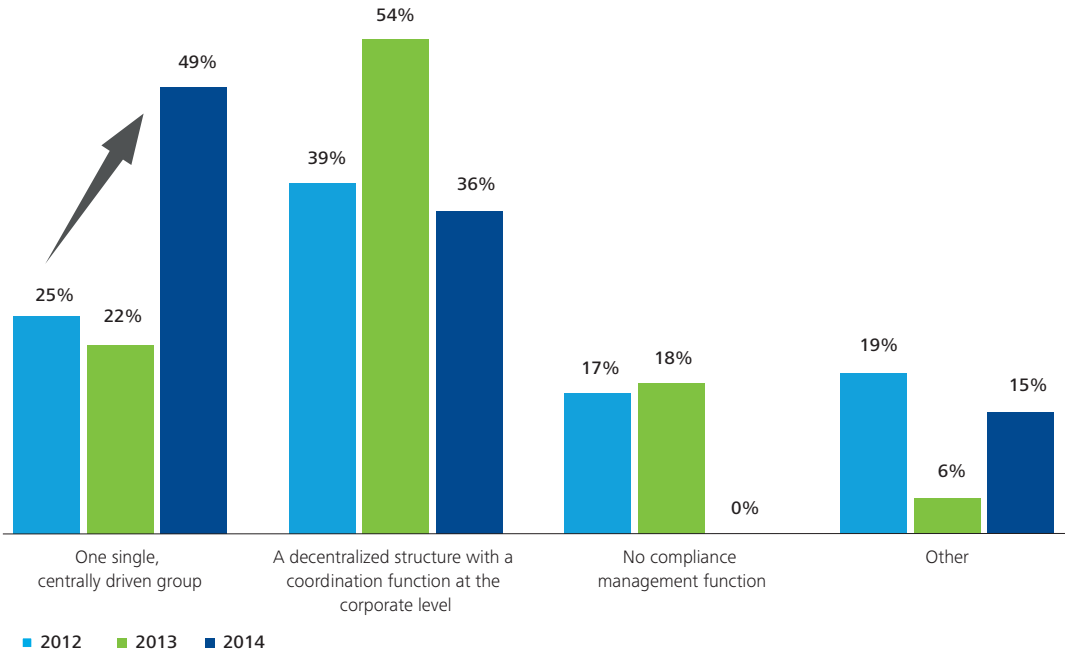


Most companies don't have a separate and distinct annual budget for CFTC compliance activities, with 81 percent of survey participants indicating that funding for CFTC compliance is embedded in their overall operations budget. Spending for Dodd-Frank compliance varies, with 42 percent of the surveyed companies reporting costs-to-date of less than $500K and the remainder reporting costs-to-date of $500K or more. Only 38 percent expect to spend more than $1M total preparing for Dodd-Frank.

CFTC compliance is increasingly centralized

The biggest change in this area is that all respondents now have a compliance management function and the number of companies that have centralized oversight of CFTC compliance has nearly doubled over the past two years to 49 percent. This is a significant increase, but it is not surprising.

Figure 19: Which of the following descriptions apply most to your CFTC compliance oversight function?



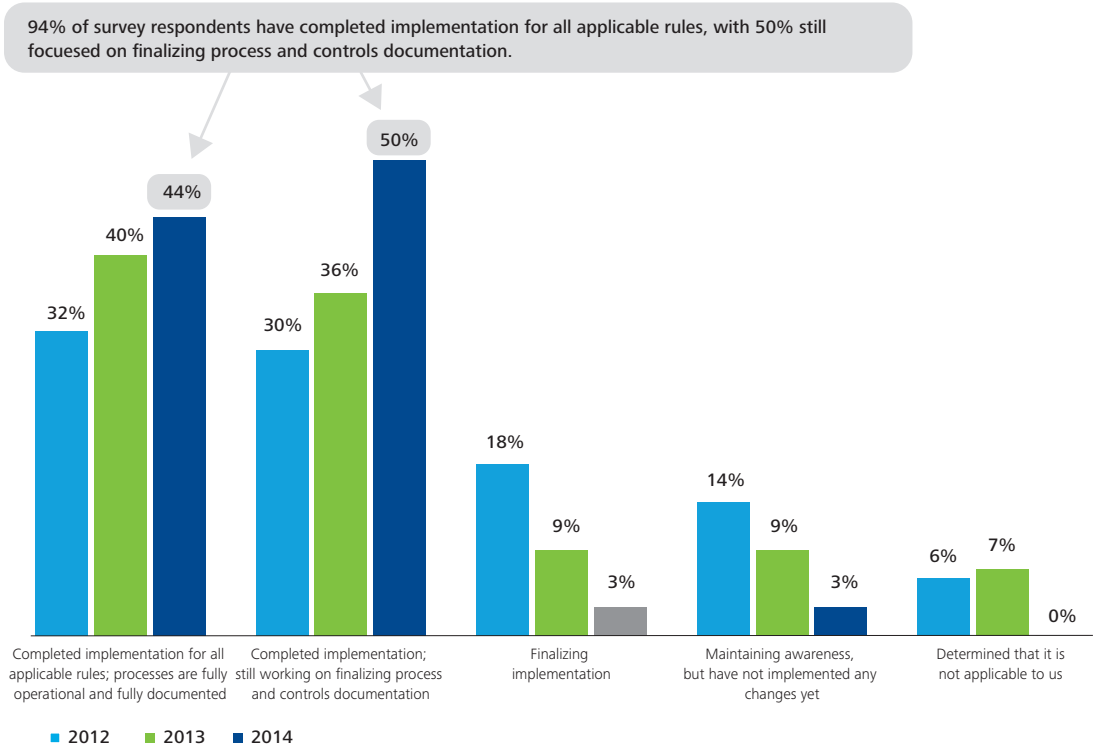
Moreover, 67 percent of the companies with a centralized group for CFTC compliance say the function is fully independent from operations. These trends are generally consistent with Dodd-Frank's transition from preparation to execution.

source: www.cftc.gov

Dodd-Frank in action

This year's survey results show that 94 percent of participants have completed implementation for all applicable and final Dodd-Frank rules. However, 50 percent are still finalizing their documentation of processes and controls.

Figure 20: How would you characterize your current approach to the implementation of requirements associated with Dodd-Frank?

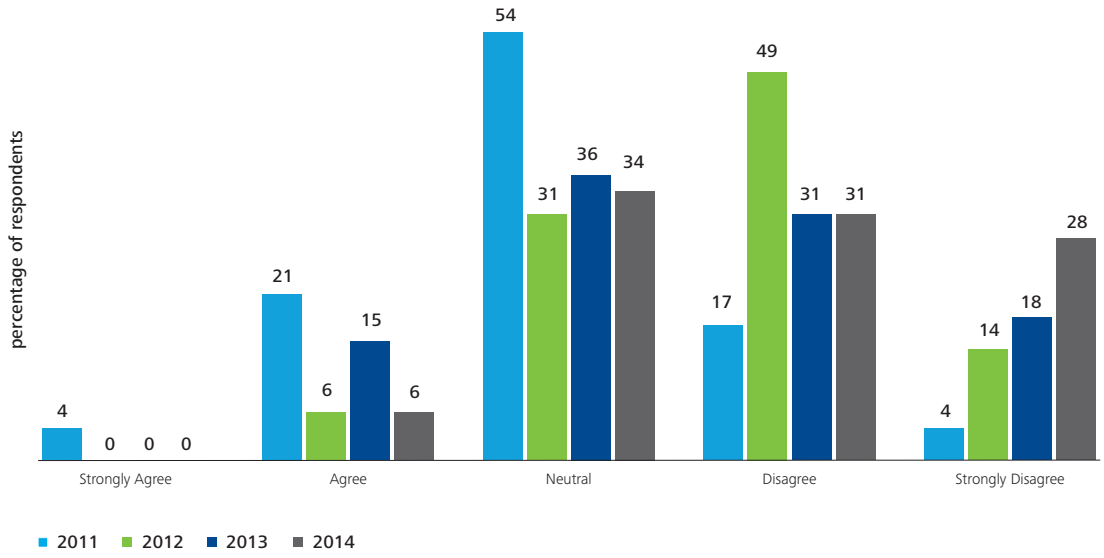


Half of the surveyed companies have formed a monitoring and surveillance group to support Dodd-Frank compliance, typically staffed with 1-2 full-time employees (FTEs). The top three challenges cited in this area are: (1) position limit reporting, (2) real-time reporting, and (3) data and recordkeeping.

Lack of clarity remains an issue

The CFTC now oversees roughly 2,000 energy companies, many of which have little or no experience with the commission and are still trying to figure out how it operates and enforces rules. When asked if CFTC regulations are clear and understandable, 34 percent of survey participants were neutral, while 59 percent disagreed or strongly disagreed - a 10-point increase over 2013. Primary challenges include: complex/unclear definitions, voluminous regulations, frequent changes to the regulations, and difficulty applying Dodd-Frank to the energy industry. Additionally, much of the actual "nuts and bolts" of the regulations have been put forth in no-action letters or other explanatory letters from CFTC staff, rather than formal guidance, which requires incremental effort to assess or dependence on outside advisors.

Figure 21: Regulation by the CFTC is clear and understandable.



Key takeaways

- **Manage uncertainty.** For most energy companies, the financial and operational impact of Dodd-Frank compliance has flattened out to become more of a maintenance or "business as usual" activity rather than an area of significant new investment. However, according to the survey results, the CFTC's regulatory requirements seem to be more complex and less understood than those from NERC and FERC. Organizations should be prepared to face continued uncertainty, even as they seek additional clarity on the CFTC's requirements and expectations.
- **Continue to prepare for increased enforcement / scrutiny.** The CFTC continues to make efforts to enhance its monitoring, surveillance and enforcement capabilities. Even as the commission appears to be taking a more pragmatic view of "end-users" in many areas of Dodd-Frank, the focus on market manipulation and disruptive trading practices continues to increase and have broader reach. As such, having a more robust and centralized monitoring and surveillance capability will likely become increasingly important over time. Companies should consider leveraging efforts already underway related to FERC compliance to gain efficiencies in building these types of programs.
- **Transition to "business as usual".** As noted above, most companies have completed the vast majority of the implementation work related to Dodd-Frank requirements. However, the level of process and controls documentation is still lagging. As companies move from "project to process" and new personnel transition into the operational roles, having strong process and controls documentation, as well as training becomes increasingly important as an area of focus.

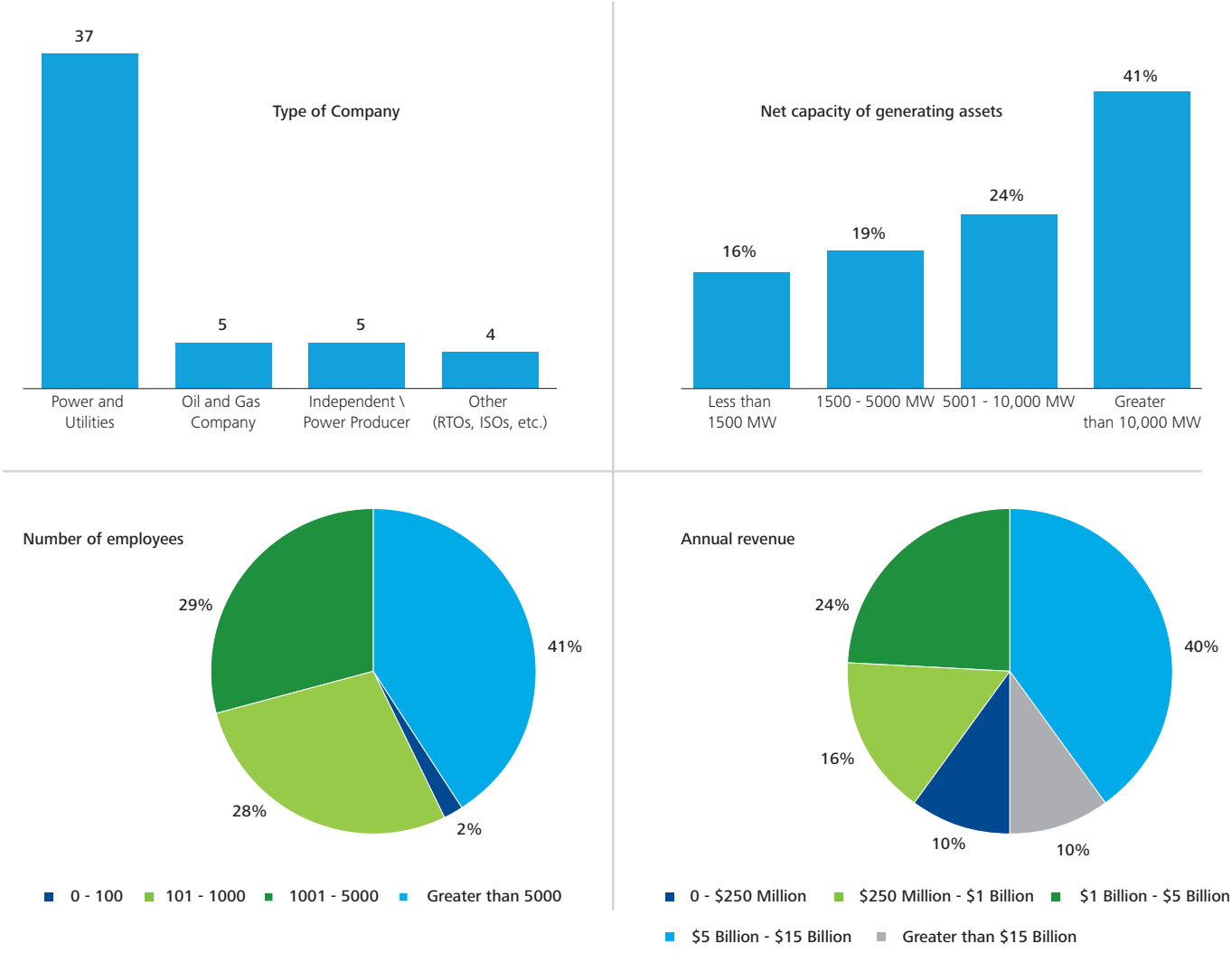
Conclusion

The regulatory environment for the energy sector continues to evolve and remains very dynamic in key areas. This creates uncertainty and a need for constant monitoring and sufficiently nimble response capabilities, making it difficult for some companies to optimize their approach for sustained compliance. Will regulations continue on their current trajectory, or will changes in regulatory focus and leadership lead to new requirements and expectations? As is often the case, that is impossible to know. What's important is to keep your eye on new developments, have effective controls for tracking and response while making a conscious effort to adequately understand both the regulatory and relative risk landscape.

About the survey

This year's survey was conducted between November 2014 and January 2015, and included 51 US energy companies representing every major region and industry sub-sector, from oil and gas to Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs).

Figure 22: Demographics



Contact information

For more questions about this document or regulatory compliance issues related to your company, please contact:

Howard Friedman (Houston)
Energy and Resources
Deloitte & Touche LLP
Phone: 1 713 982 3065
Mobile: 1 630 215 7564
E-mail: hfriedman@deloitte.com

Paul Campbell (Houston)
Energy and Resources
Deloitte & Touche LLP
Phone: 1 713 982 4156
Mobile: 1 713 503 6993
E-mail: paulcampbell@deloitte.com

Matthew Barbera (New York)
Energy and Resources
Deloitte & Touche LLP
Phone: 1 212 436 3487
Mobile: 1 646 208 3379
E-mail: mabarbera@deloitte.com

Upon request, we can meet with you to discuss how your responses compare to the responses in the overall survey and/or other specific grouping(s) of companies (assuming there are enough responses to maintain anonymity).