Introduction

For energy companies, the regulatory landscape continues to ebb and flow, remaining as diverse as ever across both commercial and operational activities, substantively complex and fragmented with each passing year. As the breadth of regulatory obligations continues to expand and regulators’ expectations continue to rise, energy companies are increasingly feeling more pressure to have in place programs that truly support operational compliance in an atmosphere where uncertainty often exists around the level of authority of federal, state, and local regulators over compliance responsibilities.

The energy industry has faced extensive regulatory changes and heightened expectations from regulators and the public alike. Today, this is coupled with rapid technological transformations in the operational landscape including increasing investments in renewable energy resources supported by rapid deployment of distributed energy resources (DERs), including energy storage and smart grid management systems. Additionally, over the last few years, as energy companies have become increasingly “smart” and data-driven, so have the customers—who have a heightened sense of awareness of the sources of energy, which has bolstered the demand for clean energy and energy-efficient solutions. Coupled with these developments, energy companies have been subject to a number of unanticipated force majeure events that disrupt day-to-day operations. These dynamic forces in the business landscape are driving the regulatory environment and have prompted many energy companies to redesign their operations risk management strategies and rethink how they approach compliance management and oversight.

To gain insights into the changes that are occurring in the energy industry—and how companies are addressing them—Deloitte recently conducted its ninth annual regulatory compliance survey of the energy industry. The ongoing objective of the survey is to help energy companies get up to speed on the latest compliance trends and leading practices, and to provide insights about what their peers in the industry are doing to improve their compliance programs and proactively manage compliance risks more efficiently and effectively to continuously advance their compliance programs.

This report highlights key findings from the survey, which are grouped into five categories:

- Enterprise Compliance
- North American Electric Reliability Corporation (NERC)
- Federal Energy Regulatory Commission (FERC)
- U.S. Commodity Futures Trading Commission (CFTC)
- Emerging Compliance Trends

### About the survey
The in-depth survey was conducted in late 2017 and early 2018. A total of 49 companies participated, 30 of which also participated in the prior year. Survey participants included major oil companies, integrated utility companies, independent power producers, and independent system operators. Respondents included chief compliance officers, senior compliance and ethics directors, managers and specialists, and associate/general counsels (see figure 1).

### Figure 1. Demographics overview
Which description best fits your company?

- **Power and Utilities**: 33
- **Independent Power Producers**: 6
- **Oil and Gas**: 4
- **Other (RTOs, ISOs, etc.)**: 6

#### Number of employees
- 0 to 1,000: 27%
- 1,001 to 3,000: 16%
- 3,001 to 5,000: 16%
- 5,001 to 10,000: 16%
- Greater than 10,000: 10%

#### Generating portfolio
- Less than 1,500 MW: 16%
- 1,500 to 5,000 MW: 22%
- 5,001 to 10,000 MW: 29%
- Greater than 10,000 MW: 29%
- We do not own generating assets: 4%

#### Annual revenue
- $0 to $250 million: 16%
- $250 million to $1 billion: 10%
- $1 billion to $5 billion: 14%
- $5 billion to $15 billion: 33%
- Greater than $15 billion: 31%

Note: Percentages may not always equal 100% due to rounding of odd numbers, or “select all that apply” questions.
Enterprise compliance

**Proliferation of fit-for-purpose hybrid governance structures**
The current state of the industry’s regulatory landscape remains in flux, which, in turn, has resulted in energy companies increasingly designing compliance programs that are tailored to fit their existing organizational structures and unique needs. Such customization can include adjusting traditional governance models and deploying hybrid models to better meet the complex regulatory requirements prevalent in today’s marketplace.

The survey data further reinforced this trend. This year, the majority of respondents (76 percent) indicated the use of a hybrid governance model where regulatory and enterprise compliance responsibilities are dispersed among the business functions with some semblance of centralized support from a corporate compliance team (see figure 2).

This fundamental shift signals an increased sense of ownership and a collaborative culture in the workplace as compliance works closely with the frontline business owners to promote transparency and accountability and reliance on a larger population of personnel, typically dispersed throughout the organization. Such fit-for-purpose governance models enable compliance functions to not only provide oversight, but also add value to the business by developing oversight frameworks that are designed to effectively identify and reduce inefficiencies and simultaneously help reduce the risk of noncompliance.

Effective governance models deploy the use of comprehensive accountability frameworks to foster a clear understanding of roles, responsibilities, and reporting lines across the three lines of defense. The incorporation of such frameworks that clearly delineate and document the responsibilities is particularly important in the energy industry where owners of tasks may be spread across multiple and distant facilities resulting in a potential lack of coordination and thereby timely completion of priority tasks.

According to this year’s results, only half (51 percent) of the participating companies have an accountability framework that defines all key roles and responsibilities, suggesting there is room for improvement in how governance models are formalized and enacted to drive accountability while promoting transparency and collaboration for compliance management activities across organizations.
**Volume of rules and regulations directly drives corporate compliance headcount**

While a majority of the respondents (61 percent) have a formal regulatory change management program, organizations continue to appear to be challenged with managing the sheer volume and pace of change, interpreting the change, and understanding the impact to their respective organizations. Understanding the scope and impact of these rules and regulations and their impact to the organization is a common area of interest for compliance leaders to ensure the responsible enterprise compliance functions are adequately staffed with an appropriate FTE headcount. Respondents indicated that compliance executives have continued to expand their workforce FTE count, with a year-over-year increase of nearly 20 percent from the number of respondents who indicated between 5 to 20 FTEs being involved with day-to-day oversight within the compliance function. Further, the results appear to account for the growing number of compliance regulations; additional analysis showed a direct correlation between the number of corporate compliance FTEs and the number of rules and regulations under corporate compliance oversight. (see figure 3).

**Figure 3. Relationship between FTEs and volumes of rules and regulations in 2017**

How many FTEs does your company involve in the day-to-day oversight associated with the corporate compliance function, and approximately how many rules and regulations do these FTEs have oversight and responsibility over?

![Graph showing the relationship between FTEs and volumes of rules and regulations in 2017](image-url)
Compliance and business partnerships help shape a stronger culture of compliance

Compliance staff, including internal auditors, have a history of being viewed, by personnel within their organizations, as watchdogs or police officers. This may create an environment of contention, potentially resulting in political issues with authority and ownership, instead of a culture of cooperation and collaboration. Historical survey data appears to indicate that compliance organizations have been working toward changing these perceptions to establish trusted partnerships with frontline business unit employees, while still maintaining independence and objectivity. Nearly two-thirds of respondents (63 percent) now believe their compliance organizations are viewed by the rest of the business as partners and enablers, not just watchdogs or police officers—up from 55 percent in last year’s survey (see figure 4).

Figure 4. How the compliance organization is viewed
How do you think members of your company would characterize the reputation of the compliance organization?

- Business Partner/Enabler
- More of an Enabler than police officers
- More of a police officers than Enabler
- Watchdog/police officers

Over the years, compliance organizations appear to be increasingly collaborative with the business/first line of defense.
This shift suggests continued improvement in the compliance function's reputation, as well as increased collaboration with business units and the first line of defense. More importantly, this year, just under half of the respondents surveyed (41 percent) indicated their organization has a method for gauging their perception of the performance of the compliance organization as characterized in figure 4 above. This is an increase from only 26 percent the year prior with three quarters of respondents (74 percent) stating they had no method to gauge this perception in 2017.

Strong cultures of compliance tend to influence employees to do the right thing, the ethical thing, even when no one is watching. Cultivating a culture of compliance can lead to positive outcomes, including reduced noncompliance fines, higher employee engagement, and a competitive advantage when it comes to strategic commercial and operational growth. This year’s results showed that two-thirds of compliance organizations measure the culture of compliance and level of integrity across the enterprise using established gauges, such as completion of training (78 percent), employee surveys (66 percent), and the types of calls that come into the hotline/helpline (66 percent). This appears to illustrate a positive relationship between the increase in the perceived reputation of the compliance function and its business partners as enablers, which, in turn, may help drive a stronger culture of compliance.

**Adoption of GRC tools is on the rise and the search for the right one continues**

Governance, risk, and compliance (GRC) tools are increasing in popularity as organizations seek to find tools to support enterprise-wide compliance programs, drive efficiencies, and keep pace with emerging technologies. With organizations seeking to find ways to manage policies and procedures and implement their supporting controls for multiple regulatory requirements across several business units, for many, GRC tools are often times proving to be advantageous and worth the cost. The survey results show a clear year-over-year increase in the use of more sophisticated GRC tools; however, a wide variety of software vendors are being tapped for their tools. Furthermore, overall satisfaction with existing GRC tools varies, with 62 percent of respondents being satisfied with their current tools’ capabilities and the remaining 38 percent responding that their existing tools are not meeting expectations.

In terms of budget, most respondents (64 percent) indicated to budget less than $250,000 annually to support compliance-related technologies. This year’s results show an uptick from last year in budget for new technology spend, suggesting additional investments being made in applications supporting compliance automation and management.

What is your organization’s approximate budget for maintaining ongoing support for your compliance applications (GRC, compliance automation tools, document repositories, software vendor licensing/maintenance fees, etc.):

<table>
<thead>
<tr>
<th>Budget Range</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than $2MM</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>$1,000,000 to $1,999,999</td>
<td>7%</td>
<td></td>
</tr>
<tr>
<td>$750,000 to $999,999</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>$500,000 to $749,999</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>$250,000 to $499,999</td>
<td>11%</td>
<td>6%</td>
</tr>
<tr>
<td>$100,000 to $249,999</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Less than $100,000</td>
<td>32%</td>
<td>32%</td>
</tr>
</tbody>
</table>

Note: Percentages may not always equal 100% due to rounding of odd numbers, or ‘select all that apply’ questions.
Expanded compliance requirements are driving up NERC budgets and staffing

NERC continues to be the most costly and resource-intensive compliance area explored in the survey. The sheer volume and broad applicability of NERC regulation, as well as the recent reform of the critical infrastructure protection (CIP) standards, were cited as the primary factors behind overall budget size and sustained growth.

Approximately half of respondents (53 percent) have a dedicated NERC compliance budget of $1 million to $5 million per year, and 25 percent have an annual budget of more than $5 million—up from 10 percent or less in prior years. Meanwhile, the number of energy companies with NERC compliance budgets of less than $500,000 fell from 31 percent in 2015 to just 3 percent this year (see figure 5).

FTE headcounts supporting NERC compliance activities appear to have continually increased, with a substantial increase to 50 percent of respondents now employing 11 or more FTEs for NERC compliance activities, up sharply from 24 percent in 2016 and 19 percent in 2015 (see figure 6). The demand for additional FTEs has been met primarily by leveraging internal resources, with the vast majority of companies (97 percent) reporting that fewer than 25 percent of their NERC FTEs are fulfilled by external contractors.

Figure 5. Annual NERC budgets
What is your organization’s approximate annual budget for NERC compliance-associated activities (including salaries, oversight and management activities, third-party fees, etc.)?

<table>
<thead>
<tr>
<th>Budget Range</th>
<th>2017</th>
<th>2016</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than $10,000,000</td>
<td>14%</td>
<td>11%</td>
<td>3%</td>
</tr>
<tr>
<td>$5,000,000 to $9,999,999</td>
<td>11%</td>
<td>11%</td>
<td>7%</td>
</tr>
<tr>
<td>$2,500,000 to $4,999,999</td>
<td>25%</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>$1,000,000 to $2,499,999</td>
<td>28%</td>
<td>44%</td>
<td>41%</td>
</tr>
<tr>
<td>$500,000 to $999,999</td>
<td>19%</td>
<td>18%</td>
<td>11%</td>
</tr>
<tr>
<td>Less than $500,000</td>
<td>3%</td>
<td>8%</td>
<td>31%</td>
</tr>
</tbody>
</table>

Figure 6. NERC compliance staffing levels
How many FTEs (including FTE contractors) support compliance monitoring/oversight/advisory support for NERC requirements (excluding operations personnel such as those that own the compliance risks or business processes)?

<table>
<thead>
<tr>
<th>FTE Count Range</th>
<th>2017</th>
<th>2016</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 20 FTEs</td>
<td>8%</td>
<td>32%</td>
<td>58%</td>
</tr>
<tr>
<td>11 to 20 FTEs</td>
<td>18%</td>
<td>39%</td>
<td>41%</td>
</tr>
<tr>
<td>5 to 10 FTEs</td>
<td>39%</td>
<td>2%</td>
<td>17%</td>
</tr>
<tr>
<td>1 to 4 FTEs</td>
<td>39%</td>
<td>18%</td>
<td>11%</td>
</tr>
</tbody>
</table>

50% of respondents employ 11 or more FTEs for NERC compliance activities, a notable increase from prior year results.
The costs and challenges of CIP sustainment
In an era where risks associated with the digitization of the electric grid keep people up at night and the safety of the US critical infrastructure is often a topic of discussion, it is no surprise that survey data indicated that costs and challenges associated with the sustainment of CIP v5 and v6 remain significant. The number of companies expecting to spend between $1 million and $5 million increased by nearly 10 percent since last year. At the high end, nearly 20 percent of the respondents now expect to spend more than $10 million, up from 5 percent last year.

The survey explored the specific factors that are contributing to the high sustainment costs (see figure 7). The top-rated challenge is keeping up with the onerous monthly patch management responsibilities. Close behind are the challenges associated with managing and tracking the volume of in-scope assets and devices. Finally, managing the access control requirements also appears to require heavy resource support.

Figure 7. Top challenges for CIP sustainment
Which of the following are considered top challenges in your organization’s NERC CIP V5/V6 program sustainment?

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing monthly patching responsibilities</td>
<td>81%</td>
</tr>
<tr>
<td>Managing/tracking in-scope assets and devices</td>
<td>64%</td>
</tr>
<tr>
<td>Talent supply and market availability of technical skill sets</td>
<td>61%</td>
</tr>
<tr>
<td>Managing access control to in-scope assets and devices</td>
<td>61%</td>
</tr>
<tr>
<td>Maintenance of technologies supporting NERC compliance</td>
<td>50%</td>
</tr>
<tr>
<td>Managing increased volume in background checks/PRAs</td>
<td>8%</td>
</tr>
</tbody>
</table>
FERC & CFTC

**FERC and CFTC compliance resource commitments stabilize**

Although FERC and CFTC’s active approach to enforcement and fines have amassed significant attention in the past, the underlying regulations and requirements have not changed much. In some instances, the anticipated regulatory change in the FERC and CFTC environments has been delayed, remains pending, or has been partially or completely dismissed by the administration. As a result, most of the surveyed companies seem comfortable with their existing resource commitments and investment in these two areas. For the vast majority of companies, FERC-related compliance activities, budgets, and staffing levels have remained relatively flat over the past three years. According to this year’s survey, approximately two-thirds of respondents (66 percent) continue to have fewer than five FTEs working on FERC compliance activities.

Similarly, the vast majority of respondents (84 percent) have annual FERC budgets of less than $2.5 million, and 38 percent have FERC budgets of less than $500,000 (see figure 8). In addition, nearly 80 percent of respondents indicated no change or a decrease in the company’s budget for FERC compliance oversight activities over the past 12 months.

**Figure 8: FERC compliance staffing levels**

How many FTEs (including FTE contractors) support compliance monitoring/oversight/advisory support for FERC requirements (excluding operations personnel such as those that own the compliance risks or business processes)?

Approximately 60% of respondents continue to employ **1 to 4 FTEs for FERC compliance**, relatively consistent with prior years.

The correlation in the FERC and CFTC compliance related headcount appears to cascade to the respective budgets as the vast majority of respondents (84 percent) have annual FERC budgets of less than $2.5 million, and 38 percent have FERC budgets of less than $500k. (Figure 8). Similarly, over 67 percent of the respondents dedicate an annual budget for CFTC compliance of under $500k; and 59 percent indicated the use of an active trade surveillance system.
Respondents indicated a similar sentiment when surveyed on CFTC compliance (see figure 9). Today, the vast majority of energy survey participants (81 percent) continue to employ fewer than 5 FTEs for CFTC-related compliance activities.

**Figure 9. CFTC compliance staffing needs**

How many FTEs (including FTE contractors) are involved in determining compliance with CFTC requirements (including monitoring, oversight, and advisory support)?

<table>
<thead>
<tr>
<th>Year</th>
<th>More than 20 FTEs</th>
<th>11 to 20 FTEs</th>
<th>5 to 10 FTEs</th>
<th>1 to 4 FTEs</th>
<th>Less than 1 (no dedicated resource)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td></td>
<td>3%</td>
<td>8%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td>6%</td>
<td>82%</td>
<td>12%</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td>4%</td>
<td>70%</td>
<td>15%</td>
<td></td>
</tr>
</tbody>
</table>
Emerging compliance trends

Existing and emergent digital technologies are continuing to drive change and transform the ways organizations conduct business and are creating new risks and opportunities for energy companies—not only in terms of how they operate, but also how they manage and execute compliance activities. Emerging compliance trends is a new section that was added to the survey this year to explore trends driven by the cutting-edge technological advancements across the industry, including cybersecurity, smart grids, blockchain, and robotic process automation, to understand how they are shaping the future of compliance across the energy industry.

Cybersecurity

Cybersecurity remains a key focus for regulators in the energy industry. The physical and cyber infrastructure core to the operations of most energy organizations has been long viewed as a vulnerable target for those wanting to do harm to the United States and its energy companies alike. In today’s business environment, dialogue around concerns of the security of the electric grid has been inarguably increasing. As an industry, dialogue around concerns of the security of the electric grid is inarguably increasing. With the stakes so high, it is not surprising that many companies are now increasingly seeking to proactively protect both themselves and consumers from the disastrous consequences of a compromised grid, including the compliance implications of any such event.

According to this year’s survey, 67 percent of respondents either have or are implementing an independent compliance governance program with formal processes and controls for cybersecurity. Another 13 percent believe such a program is necessary but have not begun to implement it. In addition, 85 percent of surveyed organizations have a formal framework that defines and identifies the key cybersecurity roles and responsibilities to help instill ownership and accountability.

Cybersecurity risks have two dimensions:

01. Inherent risk, which is the level of risk that exists in the absence of any controls, and
02. Residual risk, which is the level of risk that remains even after controls have been taken into account. Survey respondents rated data security and privacy, patch management, and identity access management to be the cyber risk areas with highest inherent and residual risk (see figure 10).

Figure 10. Top cyber risks for energy companies

Which of the following cybersecurity focus areas are considered to have high inherent risk (i.e., in the absence of controls) versus high residual risk (i.e., in the presence of controls) by your organization?
**Smart grids**
Over half the respondents have already begun to anticipate compliance changes related to disruptive grid technologies such as smart grids, micro grids, and distributed energy resources—with the biggest push coming from state regulators and public commissions.

Among the companies anticipating compliances changes from disruptive grid technologies: 35 percent are working with regulators and peers to identify leading practices; 18 percent already have a separate compliance budget to address the related issues (or plan to have such a budget in the next 12–24 months); and 12 percent are actively looking to hire people with expertise in this area.

From a regulatory and governance perspective, advanced metering infrastructure (54 percent), physical and cyber security regulations (46 percent), and distribution automation for grid reliability (43 percent) appear to be the top areas under the smart grid lens (see figure 11).

**Figure 11. Top priorities for smart grid focus**
Which of the following smart grid focus areas are considered to be top priorities at your organization from a regulatory compliance and governance perspective?

<table>
<thead>
<tr>
<th>Focus Area</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Metering Infrastructure (AMI)</td>
<td>54%</td>
</tr>
<tr>
<td>Physical and cyber security regulations</td>
<td>46%</td>
</tr>
<tr>
<td>Distribution Automation for Grid Reliability</td>
<td>43%</td>
</tr>
<tr>
<td>Third-party and vendor risk management</td>
<td>34%</td>
</tr>
<tr>
<td>Transmission Automation for Grid Reliability</td>
<td>31%</td>
</tr>
<tr>
<td>Consumer Empowerment</td>
<td>29%</td>
</tr>
<tr>
<td>Integrated Platforms</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Robotic process automation and blockchain**
Robotic process automation (RPA) and blockchain are two of today’s hottest disruptive technological forces, though many organizations have limited direct exposure as of yet. According to survey results, in the realm of compliance, 74 percent of respondents currently do not see the value of using RPA in the areas of corporate and regulatory compliance, and 87 percent do not see the value of using blockchain.

While respondents indicated that RPA and blockchain technologies have limited value at this time, the survey also explored areas where organizations feel these technologies may have the highest potential. Results indicated that a majority of the respondents see the highest potential for RPA application in managing and testing compliance controls (52 percent) as it automates and streamlines repetitive processes; and blockchain for third-party and vendor risk management (54 percent) due to the additional security and automation offered by the distributed ledger technology. The limited adoption of RPA and blockchain technologies in the energy regulatory and compliance landscape is potentially due to an, insufficient understanding of how these technologies work, what the ultimate value is within the compliance space, wanting to see what successes early adopters are able to achieve, and what the costs are to adopt and implement these technologies.
Conclusion
The complexity and rapid pace of change in the marketplace and the regulatory environment continue to present uncertainties for energy companies that are directly influencing how they are shaping their operating models. Energy compliance executives must make a conscious choice about how to adapt to and manage these changes while also providing value back to their organizations. As risks facing the industry continue to grow and become more intertwined, organizations must keep a finger on the pulse on emerging developments while continuing to improve their existing compliance programs and maintain a keen focus on their long-term compliance management approach. Organizations must remain vigilant and focus on strengthening how they measure and monitor the compliance atmosphere while doing their best to ensure appropriate controls are in place. Such actions will prove critical to protect organizations from new threats that are within their control to mitigate and optimize their compliance program capabilities to pivot and adapt to the needs of their companies’ strategies.

Contacts

Howard Friedman (Houston)
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 713 982 3065 and +1 630 215 7564
hfriedman@deloitte.com

Paul Campbell (Houston)
Partner
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 713 982 4156 and +1 713 503 6992
paulcampbell@deloitte.com

Matthew Barbera (New York)
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 3487 and +1 646 208 3379
mabarbera@deloitte.com

The Center wishes to thank the following Deloitte professionals for their contributions and support:

Sam Douglas Finn
Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Raghav Mathur
Consultant
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Zach Dressander
Senior Marketing Specialist
Regulatory & Operational Risk
Deloitte Services LP
The Deloitte Centre for Regulatory Strategy is a powerful resource of information and insight, designed to assist financial institutions manage the complexity and convergence of rapidly increasing new regulation.

With regional hubs in the Americas, Asia Pacific and EMEA, the Centre combines the strength of Deloitte's regional and international network of experienced risk, regulatory, and industry professionals — including a deep roster of former regulators, industry specialists, and business advisers — with a rich understanding of the impact of regulations on business models and strategy.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this document contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.