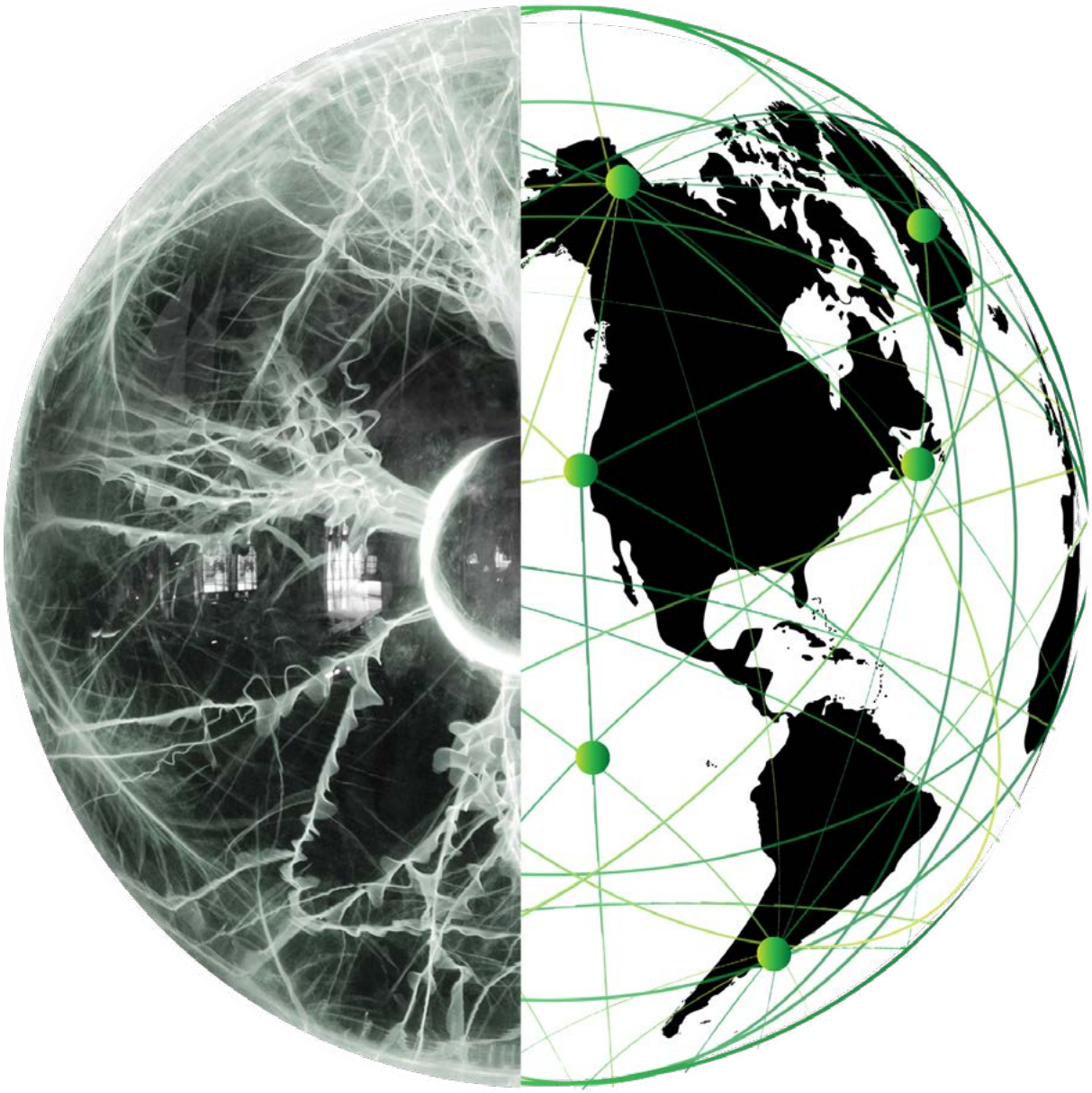
Deloitte.



Energy regulatory outlook 2020

Get started

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Contents

This publication is part of the Deloitte Center for Regulatory Strategy, Americas' cross-industry series on the year's top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients' businesses in 2020. The issues outlined in each of the reports provide a starting point for an important dialogue about future regulatory challenges and opportunities to help executives stay ahead of evolving requirements and trends. For 2020, we provide our regulatory perspectives on the following industries and sectors: banking; capital markets; insurance; investment management; energy, resources, & industrials; life sciences; and health care. For a view of the other trends that affect insurance in 2020, we encourage you to read the Deloitte Center for Financial Services companion paper.

We hope you find this document to be helpful as you plan for 2020 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.

Introduction

With the increasing prevalence and effectiveness of technology around the globe, the status quo is no longer an option. To keep up with the pace of change, the energy industry should continue evolving its approach to keep up with the myriad of challenges that it is facing, and more importantly, the opportunities that it can take advantage of in this fourth industrial revolution. Regulatory, legal, and compliance functions are being asked to do more with less, while grappling with new and emerging challenges that stem from the near-ubiquitous use of advanced technologies to meet the increasing cost pressures and need to deliver value beyond limitations with traditional approaches to testing, monitoring, analysis, and supervision.

In this digital world, new threats are emerging along with new laws and regulations to help protect consumers, the markets, and critical infrastructure. Regulators, both domestic and foreign, are focused on data privacy protections to mitigate the risks that result from improper collection, handling, storage, and use of data. Cyber threats continue to become more sophisticated and more damaging, putting even more urgency around protecting our critical infrastructure from bad actors, both external and internal.

Globalization and digital are leading to increased connection and collaboration amongst regulators around the globe. They no longer operate in silos. Instead, they look to their peers in other jurisdictions to share leading practices and learn more about how they can leverage technology, people, and processes to better monitor compliance and enforce their rules and regulations. There is also increasing coordination among regulators around the globe when it comes to the investigation and enforcement of operational and commercial behaviors and practices.

Against this backdrop, energy companies should continue to modernize and rationalize their regulatory, legal, and compliance functions and their practices. Energy companies that take a holistic view of regulatory risk management may find efficiencies that lead to streamlined and rationalized programs. A modernized compliance function can help energy companies achieve compliance as efficiently and effectively as possible by "thinking forward" and then harnessing the best available compliance practices and technologies to comply with current and future regulatory requirements. Some companies are even looking at their regulatory and compliance risk management programs as a competitive differentiator that allows them to be more nimble in the marketplace.

Regardless of how the changes wrought by lawmakers and regulators affect energy companies, it is imperative that they continue to modernize and rationalize their regulatory, legal, and compliance risk management programs so that they can meet applicable laws, regulations, and oversight and monitoring expectations in a sustainable, efficient, and cost-effective way.

Regulation enters the digital age

The energy industry is no stranger to the digital age. However, the pace of digital development is now reaching a feverish level, making it essential for organizations to focus on evolving their key business activities and managing risk. Over the past 15 years, we have seen the world continuously shift from analog to digital. Today, field operations across the energy industry value chain are collecting more data from sensors in one hour than they used to collect in an entire year. Trading has evolved from open pits filled with screaming traders to fully virtualized worlds that make it easy to trade 24 hours a day from any location that has an Internet connection. And foundational enterprise resource systems and compliance management tools are increasingly based in the cloud, changing the fundamental operating model for many companies.

Meanwhile, the sophistication of external oversight from regulators continues to grow, further highlighting the need for accelerated innovation. Regulators are already investing to improve and transform their oversight capabilities, prompting companies to reflect on their own ability to keep pace by establishing their own self-monitoring infrastructure.

Today, there are countless tools—both fit-for-purpose and open-source—that enable real-time automation, machine learning, and other previously aspirational capabilities to be more easily implemented. This has improved visibility into health, safety, and environment (HSE) risks and allowed Internet of Things (IoT) devices and data to automatically prescribe remediation. Also, it has led to trading surveillance platforms that interact with structured and unstructured data in real time to identify and, in many cases, predict trader malfeasance. It has also evolved to support the increased automation of regulatory reporting obligations that rely on both structured and unstructured data whereby the level of effort has, in many cases, been reduced by more than 75 percent through the deployment of bot technologies.

Where does your organization sit on the maturity curve, and is it where you need to be?

Learning by example

As focused case studies in a larger story line, the supply, trading, and marketing business units at energy companies provide useful examples of how these changes are taking hold. For every feature described in the trading example below, parallel opportunities can be found in other business areas across the energy industry.
Digital innovation in trading has taken many forms. Companies today have already incorporated several digital technologies into their daily activities: robotic process automation (RPA), artificial intelligence (AI), advanced analytics, sentiment analysis, and blockchain. Even as stand-alone solutions, these innovations are having an impact on how business is done. But when coordinated and combined, they begin to deliver the exponential impact so often promised by innovation. As a collective program, we call these innovations the "Digital Trade Floor."

Drilling down further, we can focus on one specific element of the Digital Trade Floor: blockchain. The widespread uncertainty and confusion that initially surrounded this breakthrough technology continues to diminish every day. Already, some companies are joining consortia and building internally facing solutions that capitalize on the distributed ledger, immutable records, and trustless environment enabled by blockchain. Meanwhile, new blockchain-related developments in cryptocurrency and tokenized assets are happening daily.

Blockchain's rapid development has grabbed the attention of all kinds of government agencies, especially regulators, who recognize the existential threat posed by virtual assets that can be transacted and settled completely through virtual currencies, potentially making fiat currencies obsolete. The Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), among others, have started asking serious questions about the broader implications of this new market and technology: Who should regulate it and how? Are the assets securities? Are cryptocurrencies just another commodity? Are existing labels and regulatory concepts sufficient? Or is a structural shift needed that reflects the new environment? Even as questions like these are being studied and debated, the energy industry is moving rapidly ahead to capitalize on the extensive benefits these innovations make possible.

Most regulators have demonstrated an understanding that major shifts are occurring, and several have already taken significant action. The CFTC made one of the first moves with its LabCFTC initiative in 2017.[1] The initiative was created to help assure the CFTC's preparedness for the impending technology changes, not only by achieving the fluency and related insight necessary to properly regulate the new innovations, but also by capitalizing on those innovations to more effectively conduct their own ongoing regulatory activities. A key goal is to improve the quality, fidelity, and efficiency of data being exchanged with and across the marketplace. According to the CFTC website, "LabCFTC is the focal point for the CFTC's efforts to promote responsible financial technology (FinTech) innovation and fair competition for the benefit of the American public. LabCFTC is designed to be the hub for the agency's engagement with the FinTech innovation community."

Since the launch of LabCFTC, regulators have been at the table when considering the benefits of implementing RPA for increased efficiency of data movement. Also, blockchain consortia could include regulators as a node to automatically provide them with access to real-time transactional data, enabling vastly improved transparency and the use of AI to generate new and deep insights about improprieties in the marketplace.

The Department of Energy (DOE) has also demonstrated a strong commitment to digital innovation.[2] In 2017, the DOE issued a million-dollar grant to a blockchain development company that is piloting mechanisms to transform the centralized electrical grid into a decentralized, distributed system of microgrids and nanogrids.[3] This potentially game-changing innovation could turn a vast collection of diverse electrical assets—including distributed solar, electric vehicles, and battery storage solutions—into a viable disintermediated network that can balance itself in real time. After its initial investment in 2017, the DOE has invested a total of $4.8 million with additional technology firms, academic institutions, and energy companies.

Looking ahead

The examples above are just a subset of the trends that are occurring as the energy industry continues to adopt digital innovation. As regulatory certainty in this area develops further (and as technologies continue to advance) the market will have even greater opportunities to realize the benefits of digital innovation—on a much larger scale.

There will undoubtedly be hurdles on the path to adoption. For example, regulator concerns about information governance and security could further inhibit the energy industry's migration to cloud, leading to data-scalability challenges. The good news is that the energy industry's digital transformation is still in its early stages, and there are still numerous opportunities to help shape the future regulatory environment.

One advantage of being an early adopter is that it enables an organization to take the journey with regulators, rather than against them—and to get involved in industry initiatives that are laying the groundwork for the future. By staying plugged in to the latest developments—and crafting a well-thought-out transformation plan—a company can position itself to capitalize on opportunities and stay on the positive side of digital disruption.

Let's talk

Mike Prokop
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mprokop@deloitte.com

Charlie Sanchez
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
chasanchez@deloitte.com

1. US Commodity Futures Trading Commission, "LabCFTC Overview," www.cftc.gov/LabCFTC/Overview/index.htm
2. US Department of Energy, "Innovation," www.energy.gov/science-innovation/innovation
3. US Department of Energy, "Department of Energy Announces $95 Million in Small Business Research and Development Grants," www.energy.gov/articles/department-energy-announces-95-million-small-business-research-and-development-grants

Digitization of regulatory compliance processes

As energy companies adapt their business models to fit today's fast-paced market environment, their legal and compliance functions must adapt as well. Digitizing regulatory compliance processes and leveraging enterprise data to monitor compliance allows the legal and compliance functions to support new business models that can help the company remain competitive in the marketplace. Also, standardizing processes through digitization can drive significant operating efficiencies and reduce the time required to complete tasks, enabling the legal and compliance functions to spend more time on strategic initiatives and proactively managing regulatory risk.

Digitization offers a set of adaptable capabilities that can be combined and built upon to help solve real problems and improve functional and process efficiency using technology. By simplifying and automating regulatory compliance processes, digital technologies can help reduce the legal and compliance functions' administrative burdens and enable managers and staff to refocus their time and effort on generating deeper insights that can help the business navigate risk more effectively.

Challenges often faced by legal and compliance organizations in the energy industry include:

- Inefficient processes
- Inconsistent reporting
- Pressure from regulators
- Insufficient resources
- No sense of ownership
- Inability to track progress on actions
- Lack of real-time information
- Human error
- No single source of truth

Digital enablement of regulatory and compliance monitoring processes can help address those issues through a unified solution.

Specific opportunities for digitization include:

- Using *automation* to reduce or eliminate the need for human involvement in repeatable tasks, which can be a major time-saver
- Using *analytics* to turn the rich data generated by digitization into valuable business insights
- Providing an improved *user experience* that boosts productivity and helps overcome resistance to change

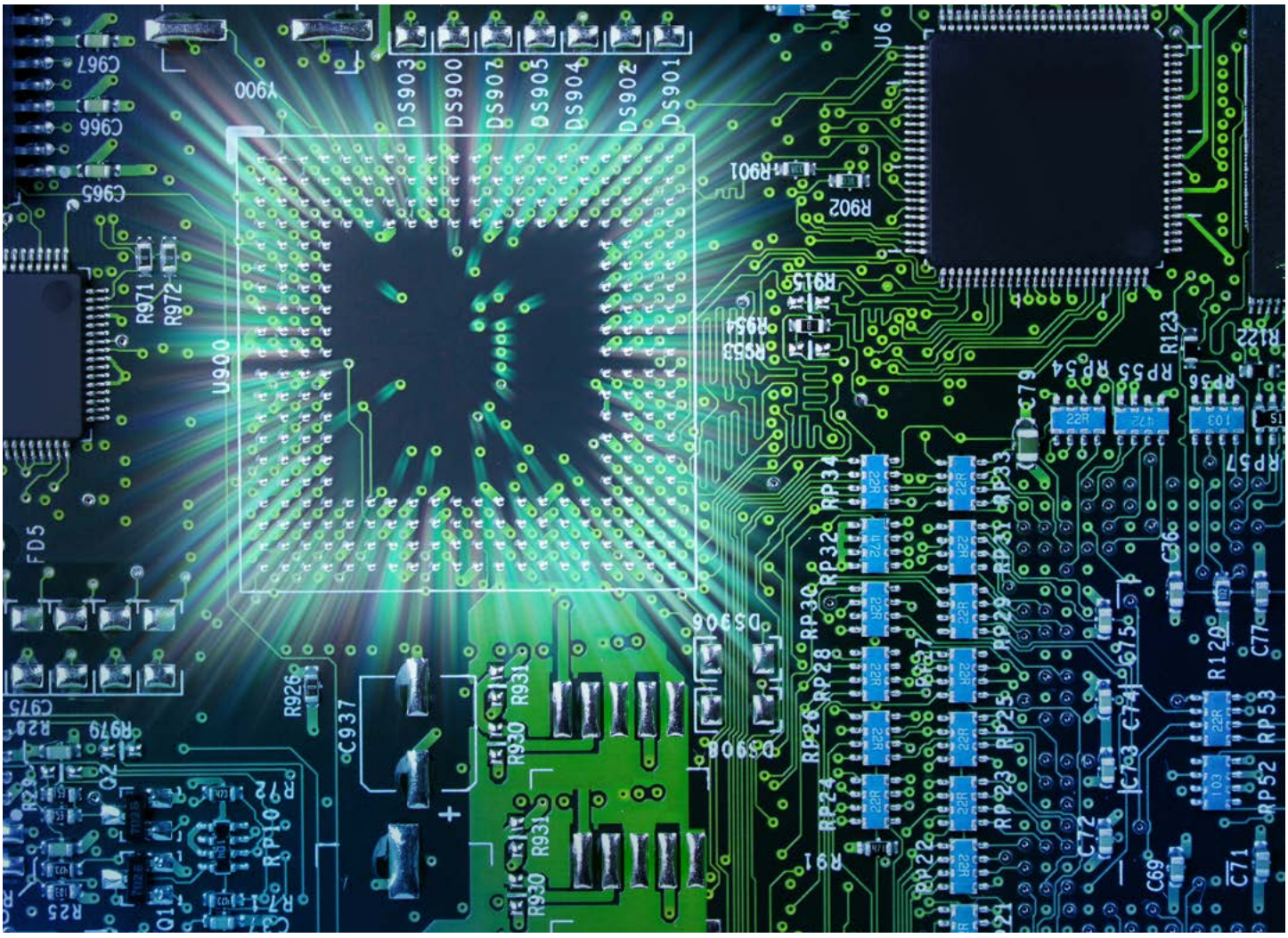
The latter is particularly important, since digitization is only impactful if it is well received and adopted by end users, including attorneys, paralegals, and compliance staff.

Getting started

The future of regulatory process management and compliance monitoring is digitally enabled. Start by inventorying current processes, prioritizing them for digitization, and then identifying solutions that support an integrated compliance framework with efficient integration of various compliance activities across the business. Choosing the wrong solutions may result in substandard implementations and an inflexible system that cannot keep up with the ever-changing regulatory landscape. Also, engage end users in the digital transformation process early and often. This can help improve adoption of the solutions, which is ultimately the key to sustainable improvement.

Let's talk

Shuba Balasubramanian
Principal
Deloitte Risk & Financial Advisory
Deloitte Transactions
and Business Analytics LLP
subalasubramanian@deloitte.com



Cybersecurity

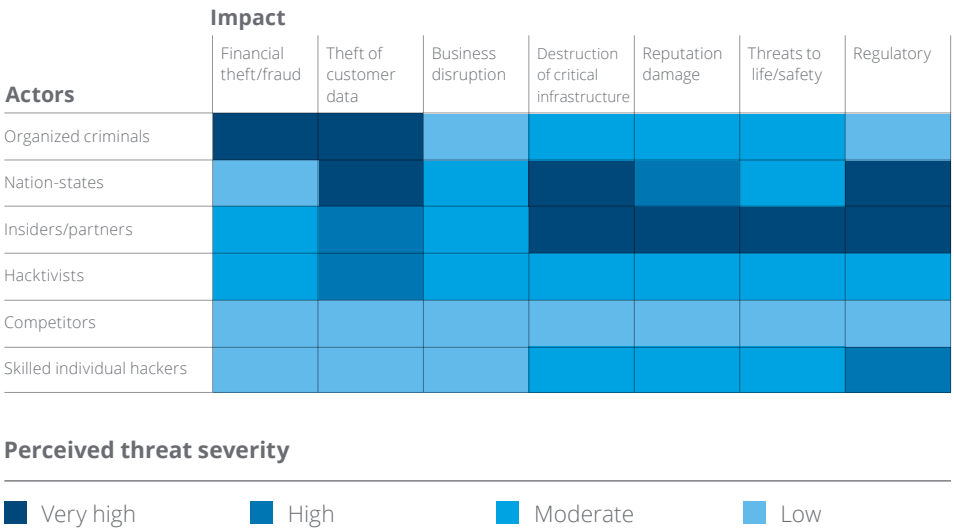
The cyber threats facing the energy sector continue to grow exponentially. According to cybersecurity experts and intelligence sources, cyber threats are not just increasing in number; they are evolving to become more intelligent and more damaging—seeking to break into the industrial control systems that operate our power grid and the systems used to move oil and gas across North America.[1] Meanwhile, nation-states and organized crime are becoming more active in this area and could be intersecting, with some experts suggesting that nation-states are now hiring organized crime groups to commit cyberattacks on their behalf (possibly as a way to deny involvement).[2] Also, hackers with little institutional or technical knowledge can increasingly access sophisticated tools on the dark web.

Figure 1 illustrates the variety of adversaries that currently pose a threat to electric grids, as an example, along with the perceived threat severity and potential impact in the United States.

To manage the impact of cyber threats and reduce the risk to the Bulk Electric System, as well as the vast network of oil & gas (O&G) transport systems, there is an immediate and continuous need to evolve the action plan for protecting existing critical and sensitive infrastructure. A key goal is to build security and resiliency into tomorrow's innovative, technology-enabled energy systems while strengthening the energy sector's cybersecurity preparedness (including incident response and recovery).

A report by the Federal Energy Regulation Commission (FERC) found that the industry is generally—but not always—meeting the standards for North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP).[3] However, there are important opportunities for improvement, particularly in two key areas:

Figure 1. Cyber threat profile for the US electric power sector is highest from three key actors



Source: Deloitte analysis

1. Further improve asset management capabilities

Traditionally, organizations have established configuration and asset management systems and tools to inventory and manage their systems, applications, devices,

software, and core infrastructure. However, in most cases, the asset information is scattered across multiple areas, lists, inventories, and systems—resulting in multiple "sources of truth" that are sometimes conflicting. Also, some organizations have started to identify services and processes that enable their business operations; yet, given the limitations of existing configuration and asset management systems and tools, they are still struggling to produce a holistic picture of their ecosystems at any given point in time.

Moreover, even when asset data is available, it is often obsolete, incomplete, or conflicting—making it incapable of supporting intelligence and actions. Also, while asset management and cyber risk have both become commonly adopted practices in one form or another, there is still very limited integration between the two disciplines.

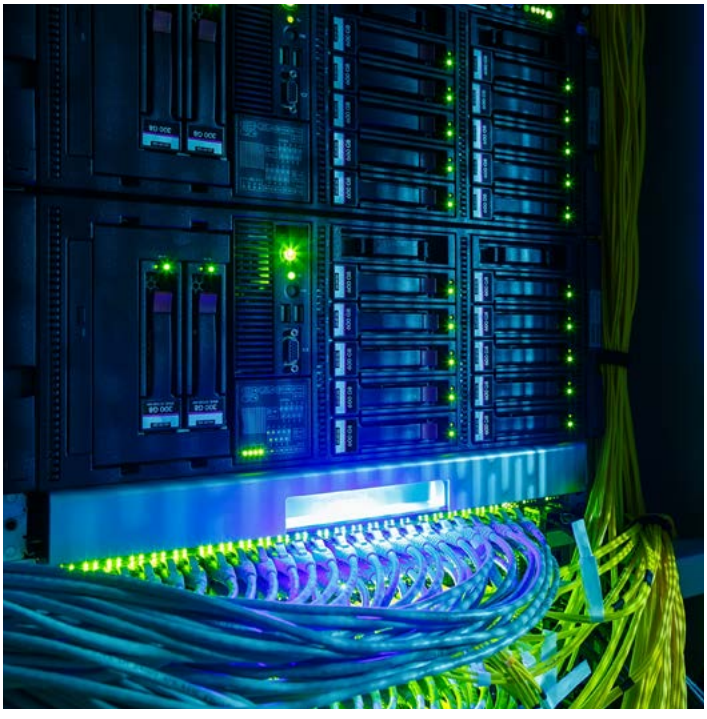
Effective cyber risk management starts with identifying and understanding risk-sensitive assets and then identifying the security controls and compliance requirements associated with protecting those assets. To understand the potential risk to a company's ecosystem, it helps to consider the key risk-oriented characteristics of each asset, including its purpose, the type of data it processes, the technology platform it is built upon, and the number of users and other people who might be affected by it. Without understanding your assets—and their significance to your business and operations—it is easy to waste a lot of time and money protecting assets ineffectively and/or protecting assets that are not important enough to warrant the investment.

2. Manage critical infrastructure risks, including safe implementation of artificial intelligence, cloud technology, etc.

As technological advancements continue to reshape the energy sector's business, operational, and cybersecurity landscape, it is becoming increasingly important to manage and evolve the critical infrastructure. The US government recently issued an executive order to strengthen cybersecurity for federal networks and critical infrastructure as a proactive defense mechanism against advanced attack vectors.[4] Known but unresolved vulnerabilities continue to present the highest cyber risk to energy companies. These vulnerabilities include using software, operating systems, or hardware beyond a vendor's support life cycle; not deploying a vendor's security patches; and failing to implement security configuration guidance/changes. All these problems can lead to exploitable weaknesses in the enterprise infrastructure.[4]

To build infrastructure that can scale with current and future energy needs, antiquated and difficult-to-defend IT should be upgraded to integrate with emerging technologies, such as cloud platforms, AI, and RPA. In recent years, the old and new worlds have been converging as established organizations embrace digital technologies and work to build the energy sector's version of the industrial IoT (including the "smart grid"). These improvements and upgrades could introduce new cyber risks if organizations do not bolster their security practices, making "security by design" a required priority.

As these systems of the future are being designed and deployed, the energy sector should proactively address and manage potential risks created by AI and automation (e.g., software or models that use algorithms with biased logic, flawed assumptions, or judgments; inappropriate modeling techniques; coding errors; poor mapping). Also, as the adoption of cloud-based platforms continues, real-time and effective management of security controls remains a challenge for many organizations. Major issues include encryption, access perimeters and portals (additional points requiring security), ownership of controls, and coordination/management of controls monitoring and testing.



Taking action

Although cyber risk is challenging to address, energy companies can start by identifying and mapping critical assets across the extended enterprise; using a cybersecurity control framework to assess the effectiveness of the control environment; and building an ecosystem that is stronger, faster, more innovative, and more resilient in the face of persistent and ever-changing cyber threats. Specific actions to consider moving forward:

- Regularly evaluate your cyber threat profile, including threat actors, the threat attack surface area, and the potential impact
- Develop and adjust your cybersecurity strategy and plans to reflect your cyber threat profile and modernization efforts (business, operational, and technology)
- Ensure the cybersecurity team has a seat at the table with decision-makers from business, core operations, and technology
- Adopt and integrate NERC CIP and cyber risk management principles for security into your organization's security program (including physical security)
- Assign ownership to design, implement, and execute security processes—providing appropriate and regular training
- Design and regularly test the effectiveness of your cybersecurity resiliency processes, adjusting them as needed to accommodate changes to your business, core operations, and technology
- Collaborate with external entities to learn, prevent, and improve your readiness to handle adverse events

Sharing intelligence, lessons learned, new solutions, and technology ideas can help the energy sector protect itself from cyber-related disruptions while at the same time improving and modernizing its business and operational models and methods.

Let's talk

Sharon Chand
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
shchand@deloitte.com

1. National Cybersecurity and Communications Integration Center, *FY 2016 incidents by sector*, www.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf
2. Lillian Ablon, "Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data," www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf, The Rand Corporation, testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, March 15, 2018, p. 6.
3. Utility Dive, "FERC cybersecurity report identifies 'potential compliance infractions'", October 11, 2019, www.utilitydive.com/news/ferc-cybersecurity-report-identifies-potential-compliance-infractions/564679
4. Executive Office of the President of the United States, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure

Recent trends in NERC CIP compliance

The FERC recently approved the latest additions to the CIP requirements, and entities registered with the NERC are now working to meet the new standards by the July 1, 2020, enforcement date.[1]

At the same time, the industry is rapidly adopting cloud services in order to take advantage of the technology innovation and efficiencies that cloud platforms can deliver. However, the current regulatory landscape presents challenges for cloud adoption related to regulated assets, prompting the industry to consider how changes can be made to balance energy security with innovation.

These changes are taking place against a backdrop of increased threats and threat vectors to the energy system supply chain—including insertion of counterfeit components in critical systems, poor vendor manufacturing processes, and increased use of third-party vendors.

The three recently updated CIP standards apply to assets rated high- and medium-impact based on the NERC criteria, including assets such as control centers and certain substations and generation stations. Overall, these updates represent some of the most broadly reaching standards to date in the affected business areas, which include areas that have not traditionally had CIP responsibilities, such as supply and procurement, third-party vendors, system integrators, and software providers.

- **CIP-013 / Cyber Security – Supply Chain Risk Management (C-SCRM**) calls upon registered entities to develop documented C-SCRM plans to identify and assess risks related to vendor products; installing vendor products and software; and even transitioning from one vendor to another. In addition to requiring an overarching plan, this update explicitly identifies six key required process areas—although it does not specify how to implement them. The six areas are vendor security incident notification, coordinated vendor incident response, vendor personnel termination notification, vendor vulnerability disclosures with respect to products and services, verification of vendor software integrity and authenticity, and coordination of vendor remote access controls.
- **CIP-005 / Cyber Security – Electronic Security Perimeters** requires registered entities to uphold two new standards: identifying active vendor remote access sessions and establishing methods to disable active vendor remote access sessions. Whereas CIP-013, above, requires addressing this risk through a plan and potential procurement controls, CIP-005 specifies the technical requirement that needs to be addressed.
- **CIP-010 / Cyber Security – Configuration Change Management and Vulnerability Assessments** makes it mandatory for an entity to analyze the source from which its software originates, as well as the integrity of the software it has obtained from the source. The intent is to make it increasingly difficult for attackers to take advantage of vendor patch and software distribution practices to introduce compromises into a system.

Due to the number and complexity of vendor relationships and contracts involved—which often reach into the thousands—implementation of these changes creates a compelling case for moving away from manual, labor-intensive processes. The depth of analysis required becomes even greater when the risk comes not only from direct vendors (third parties), but from the vendors' vendors (fourth parties and beyond). In these situations, merely illuminating the full scope of an organization's vendor ecosystem—even before assessing contracting terms and access points—will likely be a major challenge. Operating such a multitiered supply chain security program in a sustainable way will likely require automation. Although this is a new and potentially disruptive prospect for some energy organizations, there are precedents (and perhaps lessons to be learned) from industries, such as financial services, that have a history of automating vendor risk management.

Another hurdle for organizations affected by the CIP updates is the need for organizational alignment among business areas such as procurement, operations (industrial controls systems and operational technology, substation/transmission, and plant/generation operations), security, supply, legal, and compliance. These business areas will need to work together (along with third parties, and potentially fourth parties) to implement the new standards, and ownership of the overall process needs to be clear. Situations where providers cannot meet a registered entity's expectations also require processes to develop and implement controls to mitigate cybersecurity supply chain risks.

As in all security operations, the balance between containing risk and sustaining operations can be challenging. However, it may be more acute with CIP-013, because FERC has only identified focus

areas instead of imposing a specific plan of action from above. Presumably, the standard will be audited differently from one registered entity to another, based on how each entity structures and words its supply chain risk management plan.

Moving forward

Logical first steps to address these updated regulatory requirements include identifying and inventorying contracts and vendors, as well as mapping each contract and vendor to its respective business owner. Only then can readiness assessments and "health checks" of existing controls take place. Evidence—ranging from renegotiated and new vendor contracts to technical controls related to verifying the integrity and authenticity of vendor software—can help demonstrate compliance with the new requirements, which take effect July 1, 2020.

Energy companies are also working with regulators on how to advance the regulations to further embrace cloud technologies and achieve the right level of security and resiliency controls. Entities should continue to collaborate through industry forums and discussions with regulators to prioritize the specific adjustments necessary to protect the BES while maintaining effective controls.

The electric industry has worked hard to build security and resiliency into the electric grids they operate. Now, changes to the NERC standards are moving the spotlight to an equally vital risk area that is harder to see and protect than towers, cables, and substations: the code, components, and permissions that keep the grid running. The three latest CIP updates might be a new wrinkle; however, they align with the underlying principle of resilience—and the end result should help make operators more confident.

Let's talk

Sharon Chand
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
shchand@deloitte.com

1. FERC, *Supply Chain Risk Management Reliability Standards*, available at www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

Privacy

With emerging technologies spreading to the energy industry, there are rising concerns about data privacy regulations. These privacy concerns are not just the domain of the legal and compliance functions. Rather, they touch a wide range of business areas, including information technology and security, data governance and information management, sales, marketing, and digital.

It is becoming increasingly challenging for companies to stay ahead of the evolving systems landscape—especially with the regulatory demands and security threats faced by the energy industry. In the current environment, staying current and compliant requires specialized and frequently changing skill sets.

Early adopters in the industry are challenging the way everyday field tasks are executed. Data from smart meters, in-home devices, and field sensors is enabling a new generation of data scientists to identify and manage information of critical interest to individual consumers. And with emerging technologies such as IoT, AI, and cloud computing, many energy companies are shifting their focus toward creating new opportunities for business growth.

Automation, AI, and cognitive technologies are gaining traction, creating an opportunity to reinvent work roles: assigning some roles to humans, others to machines, and still others to a hybrid model in which technology augments human performance. Examples include using augmented reality glasses to improve/accelerate picking in warehouses; providing real-time feedback and support for maintenance technicians in generation facilities; and integrating with global information systems (GIS) to allow field operators to visualize the location of underground assets before they dig.

Success in meeting privacy rules and consumer expectations will require modern approaches to data architecture and governance, as well as long-term investments in data integration, cataloging, security, lineage, and many other areas. Energy companies must therefore identify the high-risk business areas—and the effectiveness of existing data protection controls—and then understand the privacy and data protection regulations applicable to their business.

In fact, the California Consumer Privacy Act (CCPA) is one of the most widely known data protection regulations, second only to the European Union's (EU) General Data Protection Regulation (GDPR).

Although GDPR is theoretically focused on the European Union, its practical impact is essentially global, with many external goods and services offered to data subjects in the European Union falling under the purview of the regulations. Key GDPR issues include cross-border transfer requirements, supervisory authority right to audit, restrictions specific to automated decision-making, and data protection impact assessments.

CCPA is primarily focused on California-based organizations that meet certain criteria related to processing and selling large amounts of personal information (PI). However, CCPA and GDPR overlap in many areas, which is creating additional compliance challenges and complexity.

Within the European Union, many member states have been focusing on data privacy and cybersecurity issues, including national cybersecurity capabilities of individual EU countries and cross-border collaboration between EU countries. Also, each EU member state is responsible for supervising the cybersecurity of critical market operators within its boundaries, including the energy industry.

Other international privacy regulations that may affect energy companies include:

- Brazil's *Lei Geral de Proteção de Dados*
- Australia's *Privacy Act*
- Japan's *Act on the Protection of Personal Information*

Understanding the challenges

The challenges associated with privacy regulations typically fall into three domains: legal and compliance, technology, and data.

- **Legal and compliance**. An emphasis on organizational accountability requires robust privacy governance, prompting organizations to review how they write privacy policies so they are easier to understand and have appropriate protections around the entire life cycle of managing personal information.
- **Technology**. Privacy requirements affect how technologies are designed and managed. The concept of "privacy by design" has now been enshrined in law through mechanisms such as the Data Protection Impact Assessment (DPIA), which is expected to become the norm across organizations.
- **Data**. Individuals and teams responsible for information management face the challenge of providing transparent oversight on data storage, journeys, and lineage. The need for a better grasp on data collection—as well as appropriate storage protocols—can help ease compliance around data subject rights.

Ultimately, data privacy should not be viewed as just a regulatory compliance exercise. Rather, it is an important opportunity for energy companies to drive business performance and growth through improved efficiency, risk management, and innovation related to data risk technologies and business practices.

Let's talk

Sharon Chand
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
shchand@deloitte.com

Jonathan Green
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jonathgreen@deloitte.com

Digitized testing and controls automation (DTCA), enterprise resource planning (ERP), and beyond

The exponential growth and disparate nature of information make it increasingly difficult for organizations to have visibility into their control environments. Yet, as energy companies become more nimble—and their operations become more complex—the need for true transparency has never been greater.

When companies embark on the digital journey, they often find the realities of dealing with more complex systems and operations make transparency difficult to achieve. Data is decentralized, organizations have competing business priorities and limited resources, and it is time-consuming to gather and test the required information. These challenges can have a significant impact on the reliability and integrity of financial statements and regulatory reporting.

To help improve transparency and manage data more effectively, a growing number of energy companies are implementing advanced systems that include sophisticated capabilities for DTCA. These capabilities enable a company to:

- Access an interactive snapshot of the entire control environment on demand, allowing the business to predict and influence its future outlook
- Continuously monitor real-time results and provide insights that can be shared with key stakeholders—with minimal effort—allowing the company to make informed and immediate decisions and process improvements in response to control issues
- Unleash the power of the control environment by seamlessly consolidating data from various systems, enabling greater transparency and boosting process efficiency and effectiveness
- Reduce the time required to meet internal control requirements, allowing a controls organization to redeploy resources to the areas of greatest strategic value and raise its profile within the business

Deciding which controls to automate

The first step in the process is to identify whether there is the capability to automate an existing control, replace an existing control with a modern automated control, or digitize the testing of an existing control.

There are three key criteria to consider when deciding which controls to automate or what testing to digitize: format, location, and volume. Controls that fit these criteria are prime candidates for automation and/or digitization.

- **Format** *(electronic data)*. DTCA is most easily applied to controls where data exists in an electronic format (e.g., stored within an application, database, or tool) or to controls that include a combination of electronic data and structured data (e.g., spreadsheets and/or templates that follow a consistent format).
- **Location** *(data from disparate sources)*. DTCA can seamlessly connect data from multiple sources and disparate technology platforms that have not communicated with each other in the past.
- **Volume** *(high volume of transactions*). DTCA generates the greatest value and ROI for controls with a high frequency and volume of activity (e.g., daily, or multiple times per day).

In addition to these criteria, it is important to review the underlying process being automated. Automating a broken or inefficient process can lead to decreased ROI and decreased risk mitigation.

Implementing digital testing and controls automation

DTCA is a journey to create a more mature control environment, so it is very common to see a mix of digitized testing and controls automation at any given moment (and it is unlikely that every control will have the ability to be automated). We often find that starting with testing makes it possible to deliver value quickly, especially in terms of completeness of coverage and risk mitigation; however, all control environments are different, so it is important to consider all aspects of DTCA for every environment.

To implement DTCA successfully, it helps to involve key stakeholders and to carefully rationalize the controls to be automated. Major steps include:

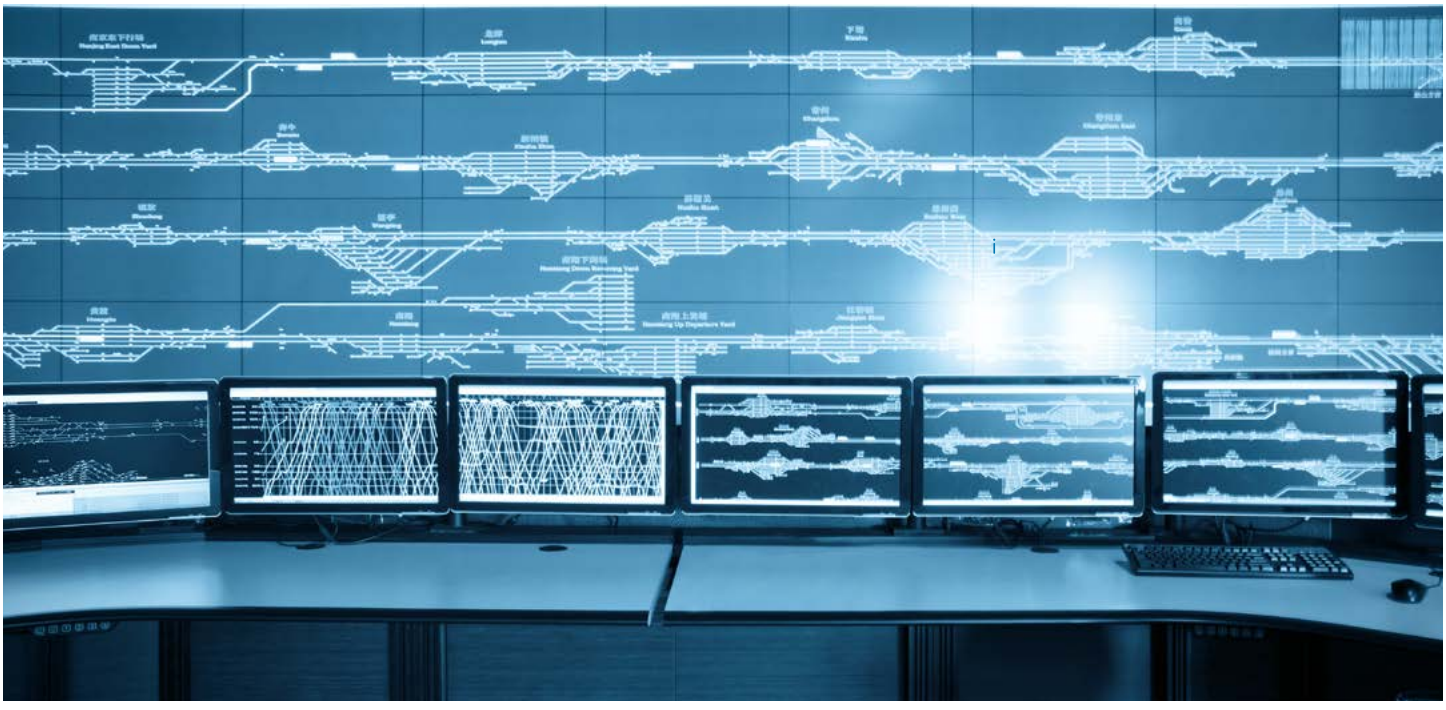
- Planning
- Assessment and validation of controls
- Automation (plan and analyze; map and extract; build and test; finalize and present)

A collaborative and thoughtful approach to DTCA implementation can deliver immediate benefits with minimal disruption to the business while also enhancing the overall compliance control environment.

Let's talk

David Rains
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
drains@deloitte.com

Tom Holland
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
thholland@deloitte.com



Supply chain

The energy sector continues to face increased risks in the areas of fraud, waste, and abuse, with risk levels fueled by the high volume of procurement spend; frequent use of consultants/subcontractors; foreign activity, including interactions with government entities; and corruption related to the awarding and execution of large contracts. Risks are further heightened by the amount of spend on large capital projects, as well as reliance on engineering, procurement, and construction management (EPCm) and other third parties to help manage a complex network of labor, materials, and specialized services.

Regulators are continuing to closely scrutinize the energy sector for problems related to corruption and fraud. The UK Bribery Act and the US Foreign Corrupt Practices Act (FCPA) are two of the major legislative cornerstones that are relied upon by regulatory bodies to enforce the diligent oversight of the supply chain practices of all industries engaged in international trade, not just the energy industry. In both the United States and Europe, there is growing regulatory interest in this space, accompanied by ongoing investigations into potential violations of these two acts. Regulators are particularly interested in red flags they believe should have alerted a company to potential wrongdoing, and they have specifically called out the lack of proactive measures and weak internal controls as failures. O&G companies tend to be at the top of the list of enforcement cases across the globe, which has resulted in ever-increasing investments by this industry in resources and technology to diligently oversee the supply chain–related activities of their companies. Regulators expect companies to have robust and effective compliance programs in place that support the auditability of the practices and the actual performance when it comes to mitigating the risk of supply chain–related violations.

Organizations around the world are adopting advanced technologies and capabilities to help detect and mitigate such red flags early. Analytics solutions based on AI can help detect potential problematic payments, relationships, and/or entities that warrant closer scrutiny—before they create significant risk or attract the attention of regulators. Similarly, proactive analytics and simulations can help address operational issues, such as how an organization's processes and controls could create vulnerabilities and how they might be strengthened. These technology-based proactive reviews can help identify unknown schemes, find undiscovered cases of known issues, and detect emerging patterns that could be problematic.

Advanced technologies can be a powerful supplement to the traditional fraud management techniques—such as fraud risk assessments, third-party contract audits, and compliance audits—that organizations have traditionally relied on to mitigate these kinds of risks. Energy companies are encouraged to review their compliance programs and build in capabilities to detect red flags early through proactive sensing—including ongoing data monitoring that can provide the level of foresight needed to take action early.

Let's talk

Larry Kivett
Partner
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
lkivett@deloitte.com

Satish Lalchand
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
slalchand@deloitte.com

1. FERC, Supply Chain Risk Management Reliability Standards, available at www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

Know your counterparty (KYC)

Over the past several years, governments and regulators around the globe have placed an increasing emphasis on combatting bribery, corruption, trade sanctions violations, and other forms of financial fraud. In 2018, the SEC collected over $2 billion in fines for violations of the FCPA.[1] At the same time, the Fraud Section of the US Department of Justice (DOJ) assessed more than $1 billion in corporate US criminal fines, penalties, forfeiture, and restitution.[2] Other regions are also increasing their efforts to prosecute corruption. Open investigations into foreign bribery allegations in Europe rose by 37 percent in 2018, and the region now accounts for more than half of all foreign bribery investigations.[3] In addition to bribery and corruption, compliance with international trade sanctions regulations is becoming increasingly difficult as the regulations evolve and change over time. To help ensure compliance with these complex regulations, and to help avoid being used as a conduit for money laundering and other forms of financial fraud, companies need a strong counterparty due diligence program.

KYC refers to the process by which businesses verify the identity of their counterparties and assess potential risks associated with establishing business relationships with them. A strong KYC process is a key element of a comprehensive due diligence program designed to protect businesses from various forms of financial fraud.

Although KYC is more often associated with the financial services industry, several laws and regulations that affect the energy industry—including the FCPA, the UK Bribery Act, and international trade sanctions—compel companies in this sector to establish strong due diligence programs. Government regulators around the world have increased their scrutiny of the energy industry, and violations of these laws and regulations carry stiff fines, potential criminal penalties, and reputational risks. In 2018, FCPA-related monetary fines assessed to corporations rose to $2.9 billion (up from $1.8 billion in 2017). Additionally, the number of FCPA-related actions brought against individuals by the DOJ and the SEC jumped to 28 in 2018 (up from 16 in 2017).[4] Much of this increase is due to the rise in cases brought against energy companies, particularly in Latin America. A strong KYC program can help companies verify the individuals that own and control its corporate counterparties and identify the potential risks they present.

Bribery and corruption are not the only risks that energy companies need to protect against. The United States, United Kingdom, European Union, and others have enacted strict trade sanctions regulations that greatly affect the energy industry. Earlier in 2019, the US Department of the Treasury announced amendments to its Venezuela-related sanctions program.[5] These amendments are specifically targeted at the Venezuela oil industry. Similar US sanctions programs against Iran and Russia continue to evolve as the relationship with these countries changes. Likewise, in the United Kingdom, the uncertainty over Brexit and its impact on the UK sanctions programs requires companies to prepare for various potential scenarios. Changes to these complex regulations make it imperative that energy companies have full knowledge of their counterparties and the transactions undertaken with them to help ensure they remain in compliance.

1. United States Securities and Exchange Commission, "SEC Enforcement Actions: FCPA cases," www.sec.gov/spotlight/fcpa/fcpa-cases.shtml
2. United States Department of Justice, *Fraud Section Year in Review 2018*, www.justice.gov/criminal-fraud/file/1123566/download
3. TRACE International, Global Enforcement Report 2018, www.traceinternational.org/ger
4. United States Department of Justice, "Foreign Corrupt Practices Act Related Enforcement Actions: 2018," www.justice.gov/criminal-fraud/case/related-enforcement-actions/2018
5. United States Department of the Treasury, "Issuance of Amended Venezuela-related General Licenses," www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190606.aspx

Establishing a strong KYC program is critical to helping energy companies maintain compliance with the FCPA, UK Bribery Act, and international trade sanctions regulations—and to helping companies better identify counterparty risk. The key elements of a strong KYC program include identifying and verifying the owners and controllers of the company's corporate counterparties; implementing a customer risk rating system that takes into consideration multiple factors, such as geographic risk, political exposure, and products and services risk; performing continuous monitoring of the company's counterparty population to identify any impacts, from amendments to trade sanctions regulations; and finally, performing a periodic review of each counterparty's risk profile to help ensure the company has current counterparty information and that the counterparty's risk remains within the parameters of the company's risk tolerance.

Let's talk

Howard Friedman
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
hfriedman@deloitte.com

Bill Maher
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
wmaher@deloitte.com

DOJ guidance on compliance programs

Earlier in 2019, two departments within the US government, the DOJ and the Department of the Treasury, published different sets of guidance on essential compliance program elements and operations.

The DOJ guidance outlines three fundamental questions for evaluating a compliance program, both to provide prosecutors with a framework to better assess the adequacy and effectiveness of corporate compliance programs and to provide corporations with insights into the DOJ's expectations for an effective compliance program from a criminal enforcement perspective. These three fundamental questions are designed to help corporations self-assess their compliance programs against the DOJ expectations:[1]

- Is the corporation's compliance program well designed?
- Is the program being applied earnestly and in good faith?
- Does the corporation's compliance program work in practice?

With these questions, the DOJ is highlighting the core elements of a corporate compliance program from a prosecutor's lens, focusing on design, implementation, and operational effectiveness. In more detail, the DOJ is advising companies to reflect on:

- **Compliance design effectiveness** and whether there is adequate focus on risk assessments, policies and procedures, training and communication, investigation processes, and third-party management
- **Compliance implementation effectiveness** and whether there is adequate dedication and commitment from senior and middle management on compliance and compliance resource management
- **Compliance operational effectiveness** and whether there is adequate focus on continuous improvement, testing, and review; investigation of misconduct; and analysis/remediation of the root causes of misconduct

About a month after the DOJ guidance was published, the Office of Foreign Asset Controls (OFAC) within the Department of the Treasury published its own guidance focused on organizations, both domestic and international, which are subject to US economic trade sanctions. Although the DOJ guidance and Department of the Treasury OFAC framework offer unique perspectives on energy compliance, they contain some similar elements.

The OFAC framework outlines five essential components of compliance: management commitment, risk assessment, internal controls, testing and auditing, and training.[2] These components allow OFAC to consider the existence, nature, and adequacy of a compliance program. OFAC may mitigate a civil monetary penalty on that basis.

- **Management commitment** is the management support a compliance program should receive and how management ensures the compliance program has "adequate resources, and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization." This aligns with the DOJ's advice on effective implementation of compliance programs.
- **Risk assessments** consist of a holistic, top-to-bottom review of the organization on a routine basis to identify potential issues that should inform policies and procedures, internal controls, and training to mitigate the identified risks. This complements the DOJ's focus on ensuring effective design of compliance programs through similar mechanisms.
- **Internal controls** provide clear expectations, define procedures and processes, and minimize risks identified by the organization's risk assessments.
- **Testing and auditing** help the organization uncover any compliance program weaknesses and deficiencies so it can identify areas for enhancement. Further, this helps ensure the operational effectiveness of programs in line with the DOJ's guidance.
- **Training** provides all personnel on a regular basis with job-specific compliance knowledge and information about compliance responsibilities for which everyone will be held accountable.

Impact of the updated compliance guidance

The DOJ guidance and OFAC framework show two different prosecutorial perspectives on the evaluation of a compliance program—and what the essential components of a compliance program should be.

Compliance professionals in the energy industry have expressed concern that the prosecuting divisions of the DOJ and OFAC are leading the charge on defining effective compliance, arguing that their guidance comes from the perspective of assumed wrongdoing.

However, the guidance should be viewed as just a starting point on the journey toward developing a leading-practice compliance program. That said, the fact that prosecuting divisions are taking the lead here should be viewed as a sign that insufficient oversight from corporate compliance programs in the past may have enabled unethical, fraudulent, wasteful, and abusive practices—resulting in criminal violation of legislative standards.

The guidance shows an increasing focus on compliance practices and infrastructure, and how the two departments plan to continue evaluating compliance programs across industries. This helps create transparency around the expected obligations of a compliance program. Currently, no other organizations have provided this type of transparency.

From a tactical perspective, the two guidance publications are complementary despite addressing different aspects of compliance and coming from different organizations. Both aim to help companies establish and sustain effective compliance programs. Also, with no other program guidance to work from, the DOJ and OFAC publications provide useful insight into how compliance programs will be evaluated in instances of criminal violations. However, the DOJ and OFAC expectations still need to be aligned and integrated with applicable regulatory obligations.

For compliance functions, the guidance shines a light on the importance of compliance and creates an opportunity to further increase the value of compliance within an organization. In particular, it helps bring C-suite attention to ethics and compliance. Also, it provides a catalyst for reevaluating a compliance program's value proposition. An enhanced compliance program can bring bottom-line benefits to the organization by helping to develop a culture of compliance and by improving the organization's reputation both internally and externally. In addition, it can help the organization become more effective by identifying and addressing issues, gaps, and overlaps within processes and procedures. This expanded value proposition can boost the C-suite's commitment to the compliance program, which can in turn be driven top-down throughout the company.

Taking action

Armed with the DOJ guidance and OFAC framework, energy companies should take stock of their compliance programs to ensure they have the capabilities in place to achieve adequate and effective compliance. Start by reviewing the two publications and assessing your compliance program at a high level against what the DOJ and OFAC deem essential. Next, conduct a detailed risk assessment of your compliance program against the DOJ and OFAC expectations, as well as the OFAC's Root Causes of Compliance Breakdowns and Deficiencies. This will provide a valuable view on how your compliance program stacks up to the guidance. Also, it can help uncover risk areas where your organization's current mitigation efforts might not be sufficient.

Whether or not you find gaps in your program during the initial risk assessment, a similar assessment should be performed periodically. This will not only help your organization prepare for any possible reviews by the DOJ and OFAC, but will also help prepare your compliance function and business units for internal and external audits, as well as other types of regulatory review. Even more important, it will give your organization an opportunity to address compliance-related issues before they become serious problems—helping to demonstrate a commitment to sustained and effective compliance.

Let's talk

Howard Friedman
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
hfriedman@deloitte.com

1. www.justice.gov/criminal-fraud/page/file/937501/download
2. www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

Staying ahead

The regulatory landscape is constantly shifting. Some changes are big enough to grab headlines. Others may be nearly invisible but can still have a big impact. For the latest regulatory updates and insights, please visit www.deloitte.com/us/EnergyRegulatoryOutlook.

Leadership

Alok Sinha
Regulatory & Operations Risk leader
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
asinha@deloitte.com

Katie Pavlovsky
Energy, Resources & Industrials Advisory leader
Principal
Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
kpavlovsky@deloitte.com

Howard Friedman
Energy, Resources & Industrials leader
Center for Regulatory Strategy, Americas
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
hfriedman@deloitte.com

CENTER *for*
REGULATORY STRATEGY
AMERICAS

About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media, including thought leadership, research, forums, webcasts, and events.

Deloitte.