Diligent

Leading From the Front:
Your Toolkit for Building a Purpose-Driven Organization

Diligent

Preparing for Climate Reporting Requirements

A Roadmap to ESG Compliance

Across the globe, climate regulations are fast approaching, and organizations are facing a series of burning questions:

"Are we prepared to share scenarios of how our operations will adapt to climate factors — including physical, legal, market and economic changes?"

"Is our company prepared to make disclosures on Scope 1, Scope 2 and, if necessary, Scope 3 impact?"

"Are we ready to do all of this in a timeline of months, rather than years?"

In March 2022, the U.S. Securities and Exchange Commission (SEC) put forward plans to require publicly traded businesses to outline the climate risks their operations bring about. Similarly, companies in the European Union must comply with increasing environmental, social and governance (ESG) obligations, with the EU Taxonomy Regulation applying from January 1, 2022. In the Asia Pacific region, the need to keep pace with peers, combined with a growing reputational risk, has led to dramatic growth in ESG reporting over the past half-decade.

What's more, across all regions, the vast majority of upcoming climate disclosures will be mandatory, not voluntary; they will likely cover both qualitative and quantitative information; and they are only a few of the sweeping changes on the horizon.

Combined with an ever-increasing investor and stakeholder focus on ESG, such developments could spell trouble for those organizations still relying on legacy systems and outdated processes for climate tracking and reporting. But specialized ESG reporting technology can offer a way forward. With the right solution in place, organizations can benefit in a number of ways — from tracking progress against ESG standards and frameworks to automatically updating compliance dashboards when new regulations arise. When it comes to scaling and maturing your ESG program, technology can integrate with your existing systems and grow with you.

Aligning SEC and ESG

With the recent SEC climate proposals dominating ESG headlines, and with those proposals likely to become requirements sooner rather than later, listed companies in the U.S. should ensure that any ESG technology solution they are evaluating can assist with the following tasks, at a minimum:

□ Outlining and documenting Scope 1, 2 and 3 emissions

□ Automatically updating compliance dashboards, reflecting new regulations as they arise

□ Monitoring third parties

□ Aggregating and collecting climate-impact data, with data sets updated automatically in real time

□ Filing accurate, up-to-date statements and reports (on greenhouse gas emissions or net-zero plans, for example), and automatically generating auditable disclosures

Climate Urgency Is Increasing in All Areas of Business

As the focus on climate grows, it can be expected to permeate businesses at multiple levels. No matter the size of the organization, the industry in which it operates or the region in which it is based, companies must now dedicate time and energy to a full understanding of emerging frameworks — and they must get a firm grasp on how to track their Scope 1, Scope 2 and, where necessary, Scope 3 emissions, as well as reporting on reductions in greenhouse gas emissions or the progress of their net-zero plan.

To put it simply, audit-ready ESG metrics are fast moving from nice-to-haves to must-haves.

New disclosure regulations will require data, processes and technology that most organizations still don’t have in place. Firms shouldn’t wait until disclosures become an obligation to establish these systems; by then, it will be too late. The best way to prepare for new disclosure requirements is to start building an ESG reporting infrastructure now.

At a minimum, organizations should be tracking:

☑ The climate impact of their business operations, such as the energy use of their buildings and the carbon footprint of their business travel

☑ The climate impact of third parties and their supply chains

But why the sudden urgency to digitally transform climate reporting? It stems, in large part, from legacy systems simply not being up to the task.

Legacy Systems and Processes Can't Keep Up with the Demands of Climate Reporting

Many climate-reporting systems used by organizations today are homegrown, several years old and highly specialized, making it difficult to add in new features and functionality as reporting demands evolve. Furthermore, few of these tools are capable of linking climate data to all of the areas in which it will have an impact. For many, this information exists in separate and disconnected systems. Coupled with outdated, often time-consuming and manual processes, this causes many organizations to find themselves ill-equipped to keep up with the rapid pace of change.

> "The importance of centralizing your climate data can't be overstated — the core benefit being able to "collect once, reuse many times." Demands from regulators will continue to grow and change, and shareholders and investors already have their own differing demands, which further complicates matters. Overloading high-value staff with the collection, aggregation and calculation of climate data for multiple frameworks using traditional workflow systems or spreadsheets is riskier and more error-prone than ever before. Only a purpose-built data collection tool built for the evolving nature of climate reporting will suffice."
>
> – Adrian Fleming, ESG Senior Commercial Director, Diligent

To understand why such inflexibility and disconnection are a problem, and why a new approach is necessary, it's helpful to look at the Task Force on Climate-Related Financial Disclosures (TCFD).

TCFD standards for climate reporting are increasingly popular worldwide and represent a new approach. Indeed, both the SEC's recent proposals and the G7 measures hew closely to TCFD recommendations, and many governments worldwide are already adopting this framework, including New Zealand, Switzerland, the U.K., China, Australia and Hong Kong. Moreover, TCFD recommendations go beyond metrics and targets to encompass governance, strategy and risk management.

Investors are requesting data of similar scope and detail as well. Whereas previously a few statistics related to energy savings and recycling may have satisfied questions about sustainability, now investors want a more holistic view of how climate links to corporate strategy and risk, with rigorous detail and tangible progress linked to promises.

Do all company operations meet Sustainable Finance Disclosure Regulation (SFDR) guidelines? Is your net-zero plan on track to meet its targets? Have shifts in return-to-work commutes and leasing arrangements altered the company's climate impact?

To answer questions like these confidently, organizations need to be able to close the data gaps between what they say they're doing and what they're actually doing when it comes to climate. They need to connect the dots between climate and business strategy. They must be able to adapt swiftly to a growing volume of disclosure demands and reporting requirements — while maintaining accuracy, productivity and efficiency.

Do all company operations meet Sustainable Finance Disclosure Regulation (SFDR) guidelines? Is your net-zero plan on track to meet its targets? Have shifts in return-to-work commutes and leasing arrangements altered the company's climate impact?

Additionally, successful climate reporting relies on a joined-up approach that is often neglected when organizations choose not to adapt their existing, siloed legacy processes. From haphazard document management to poor communication to a lack of oversight over third parties in the supply chain, the challenges that arise from an outdated approach to collecting and collating information can severely hinder the agility, speed and thoroughness that is needed for meaningful climate reporting.

> "You're going to need to be reporting on this for years to come, and reporting at an even more detailed level."
>
> – Matt DiGuiseppe, Former Vice President of Research and ESG, Diligent

As we've established, the vast majority of legacy systems and the processes that often go alongside them weren't built or designed for such work. But dedicated ESG reporting technology can be the difference between an organization simply treading water and one tackling ESG requirements head-on and thriving as a result.

With change not just around the corner but, in many ways, already here, let's take an in-depth look at how technology can help organizations to prepare for — and rise to — the ESG reporting challenges they face.

Where Legacy Systems Fall Short

Climate reporting requires a flexible, forward-looking system capable of handling a diverse array of requirements. Legacy systems fall short in a number of ways:

- They are often cumbersome and slow and are unable to interact with other systems or keep up with new ways of working
- They are often siloed, with different functionalities residing in different areas of the system
- They often don't have the functionality to keep abreast of the latest news and regulations, and don't provide insight into how peers and competitors are performing
- They fail to keep pace with the growing volume of disclosure demands and reporting requirements
- They can be expensive and time-consuming to run, diverting valuable organizational resources away from more important matters

Four Key Steps to Remaining Compliant with Climate Impact Regulations

1. Strengthen the CIO-Board Relationship

A fully realized ESG technology solution enables organizations to approach ESG with confidence. Whether it’s reporting, managing data or simply ensuring that there’s a futureproof system in place, ESG technology represents a marked step up from older systems and processes. But what capabilities should organizations look for — and why are they so important?

It goes without saying that accurate reporting is not possible without good data management. Data-rich organizations operate more efficiently, more decisively and with greater foresight than their peers — and this is particularly important when it comes to ESG.

The ESG data you collect will ultimately power the organization’s tracking, reporting and collaboration, so it’s vital to identify the right mix of internal and external data sources.

To assess your ESG data needs, start with the ESG goals you’ve laid out as an organization, as well as the frameworks you’ve selected. As you identify the data you’ll need, take time to determine where it will be sourced — whether it is internal or external. Robust external data sets can be purchased from proxy advisory or consulting firms — or even from companies like Diligent, who specialize in governance data and peer group modeling.

Given the evolving nature of ESG regulations and a rapidly changing world, make sure that your chosen solution keeps your data relevant and timely. Ideally, your data sets — whether drawing from internal departments or external markets — should update automatically in real time.

Relying on old data not only limits the visibility of your ESG performance, but it serves as a warning to investors and stakeholders that your organization is not taking its ESG responsibilities seriously.

Become committing to any ESG solution, take the following actions:

- □ Learn from your peers and competitors. Take the time to analyze their ESG processes and disclosures. Monitor the news. Keep abreast of regulatory change.

- □ Involve all relevant business units in any discussion around data. Make sure that all those involved in monitoring and reporting on ESG are aligned on KPIs and are working within the same ecosystem.

- □ Memorialize your data aggregation and collection processes and keep track of where inbound requests for ESG information are coming from.

2. Embrace Automation

Climate reporting demands are in a constant cycle of evolution. For organizations mired with cumbersome legacy systems, keeping track of those demands can feel like an impossible task. But adopting a solution that utilizes robotic process automation (RPA) can make the task much easier, simpler and far less time-consuming.

RPA automates time-intensive and repetitive tasks, running data access, reporting and remediation tasks from end to end. Moreover, it is able to integrate across disparate departments and systems, bringing old and new together so organizations can leverage their legacy technology rather than adding on more systems or rebuilding their infrastructure from scratch. From gathering, preparing and analyzing information to monitoring and reporting on data, RPA streamlines what were previously manually driven information-gathering processes into something much more seamless and much less prone to error. It is a tool that brings the right data to the right people at the right time.

Climate issues, now more so than ever, can impact operations at many levels. Before evaluating and selecting any RPA technology solutions, make sure to take the following steps:

□ Build a list of time-consuming, repetitive tasks in your climate-related operations. One place to start is with the spreadsheets teams use on a daily or weekly basis.

□ Calculate how much time staff currently spend manually collecting and analyzing data — and troubleshooting issues — in these areas.

□ Consider the accuracy of your climate reporting, both internal and external. Where are you least confident that teams are collecting the most up-to-date, relevant data?

□ Identify your biggest pain points in climate-related data collection and analysis. Deadlines? Document versioning issues?

□ Map the problem areas above against the goals of individual teams and the entire organization.

3. Monitor and Report

Are your ESG initiatives meeting expectations, deadlines and commitments? Is data being consistently disclosed across stakeholders and frameworks? An automated ESG solution can help boards and executives keep their fingers on the pulse of activities and progress — and spot red flags before they escalate into bigger issues.

A dashboard, particularly a customizable one with real-time data, can give your organization visibility into KPIs, metrics and commitments. Automated monitoring can help ESG teams sift through mountains of information in a fraction of the time.

When telling your ESG story, it's important to remember that no organization needs to start from scratch. ESG is a broad umbrella: Take inventory of the impactful activities your organization is already doing as a starting point.

As regulations continue to evolve, organizations must also make sure that their ESG reports are meeting expectations, deadlines and commitments. Look for a technology solution that can automatically generate auditable disclosures from your ESG data and dashboards. In the months and years ahead, it will be increasingly important to make sure that all changes and values are tracked for a robust audit trail. The ability to prepopulate ESG assessments with existing data not only makes the process more efficient, but easier to refer to when needed.

Before committing to any ESG solution, ensure that:

□ The ESG technology platform you choose makes reporting seamless, with reporting and data collection capabilities located under one roof.

□ The platform can aid you in communicating your ESG progress in a compelling way, helping to ensure stakeholders get the message. Ensure key talking points extend across proxy materials, sustainability reports and your conversations with investors.

4. Enable Adaptability and Scalability

As months and years pass, regulations and reporting frameworks will evolve. In tandem, the operational and disclosure needs of your organization will also increase. Whereas legacy systems — cumbersome and segregated – are ill-equipped to deal with such change, an automated ESG operating system can grow with you, easily integrating with existing systems and evolving with your organization.

Given the complexities and variability of ESG tracking, monitoring, reporting and compliance, a solution that doesn't need reconfiguring and recalibrating is crucial. Different industries use different ESG frameworks and have differing stakeholder expectations. Laws and regulatory requirements vary across jurisdictions and each organization has its own people, processes and practices for managing ESG issues.

A good ESG solution must enable them to act quickly and easily, now and in the future. Boards must be able to tailor features to their specific roles, regulatory environments and reporting requirements.

Ultimately, any solution needs to accommodate an organization wherever it stands in its ESG journey — and evolve as the organization's needs evolve. Before committing to any ESG solution, ensure that it can:

- Easily track shifting investor and stakeholder expectations.

- Work with your current level of ESG maturity and grow as you do.

- Help map ESG data to your internal objectives.

Prepare Today for Tomorrow's Disclosure Requirements

A mature ESG program with the right components in place will pave the way toward seamless compliance with future disclosure requirements.

Find out more.

Diligent

a MODERN GOVERNANCE company

About Diligent

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com.

Contact Us | Info@diligent.com | **+1 877 434 5443** | diligent.com

Diligent

Best Practices for Building a Culture of Compliance: 4 Focus Areas for Strengthening Policy Management & Compliance Training

Introduction

With an evolving regulatory landscape, increased attention to political and social issues, and heightened attention to incidents and whistleblower protections, the past five years have demonstrated that merely checking the box on compliance is no longer enough. Corporations who do not take a proactive approach risk serious financial and reputational damage.

The United States Department of Justice (DOJ) has intensified its scrutiny as well. In April 2019, the DOJ published its Evaluation of Corporate Compliance Programs guidance — a significant expansion of the earlier guidance published in 2017. With more discussion regarding what effective compliance programs should achieve and what prosecutors want to see from companies under regulatory scrutiny, it is a valuable resource for compliance officers and directors who want to ensure their compliance programs satisfy regulator expectations.

On June 1, 2020, the DOJ updated this guidance document once again to reflect, as then-Assistant Attorney General Brian Benczkowski said, “additions based on our own experience and important feedback from the business and compliance communities.”

The changes, while not extensive or surprising, do indicate increased understanding by the DOJ of the variation in circumstances in which corporate misconduct occurs and the areas in which prosecutors should focus their inquiries. Specifically:

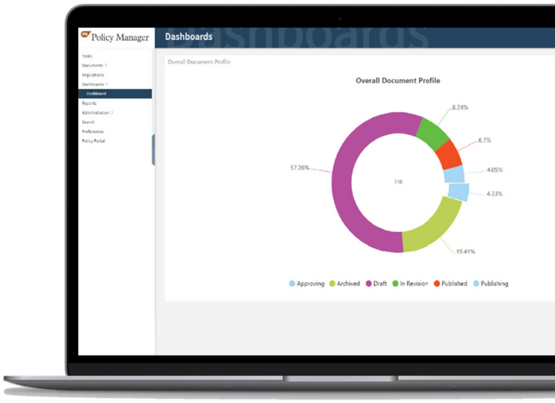
- **Is the corporation’s compliance program well designed?**
- **Is the program being applied earnestly and in good faith — adequately resourced and empowered to function effectively?**
- **Does the corporation’s compliance program work in practice?**

Internal compliance teams face many challenges in addressing these questions and adapting to a changing landscape in a timely fashion: disparate policies and processes scattered across the organization, manual processes that slow things down and employee resistance, to name a few.

Where should teams focus first?

Read on for best practices in four priority areas when building and fine-tuning an internal compliance program.

1. Policy Management



Strong, well-managed policies are the lifeblood of compliance and growth. They define, articulate and communicate expectations, communicate risk limits, explain governance and accountability, and guide desired conduct. They're essential to creating a culture of compliance, protecting the business and achieving business objectives.

Yet in today's world of rapidly changing mandates and evolving business strategies, organizations are challenged to manage hundreds or even thousands of policies. Often, these policies are scattered across the enterprise with no central repository, inconsistent styles, lack of ownership and poor lifestyle management — from insufficient mapping, to exceptions and incidents, to a lack of cross-referencing standards, rules and obligations.

If a company can't keep a firm grip on how its policies and procedures are implemented, room emerges for measures that don't reflect a commitment to strong ethics and compliance. Maybe a procedure neglects to collect a piece of data crucial for regulatory compliance. Or perhaps more nefarious practices emerge, such as putting whistleblowers on probation and nudging them out the door.

The DOJ will be taking notice. Are your policies and procedures published in a searchable format for easy reference? Does your company track access to see which policies are getting the most employee attention?

Policy Management: A Best Practices Checklist

Your organization's policy management is strong if it includes:

□ An overall policy management process in which policies and procedures relating to the compliance program are made readily available to employees

□ A "policy about policies" to ensure all are structured in a uniform way that doesn't confuse employees or third parties

□ A system of review and attestation for new or updated policies

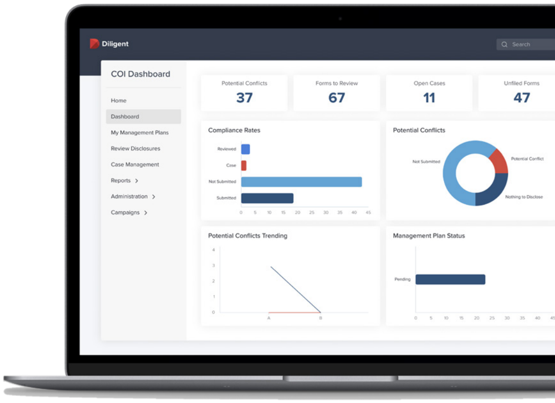
□ A thoughtful approach to exception requests, since a zero-tolerance standard can drive some parties to keep quiet about mistakes rather than speak up

□ Procedures that reflect how the business works, so employees see them as something to follow rather than something to evade

□ An integrated, streamlined policy management platform, enabling you to regularly update policies with changing regulations, track and manage employee engagement and training, and reduce your organization's exposure to noncompliance risks

□ Model and evaluate pay-for-performance plans and measure compensation according to relevant performance metrics

2. Conflicts of Interest (COI) Management



Potential Conflicts 37

Forms to Review 67

Open Cases 11

Unfiled Forms 47

Conflicts of interest are at the root of many business ethics and regulatory compliance problems. Even if a conflict isn't impermissible from a regulatory or fiduciary perspective, this conflict — whether actual or perceived — can hurt your organization's reputation. Politicians, prosecutors and the press frequently seize on COIs as suggestive of institutional malfeasance. Meanwhile, regulatory bodies such as the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), the Internal Revenue Service (IRS) and the National Institutes of Health (NIH), as well as myriad anti-corruption statutes worldwide, are increasingly requiring COI management programs.

Organizations navigating this landscape face many challenges: lost forms, employee delays and reluctance, and more. One big challenge is process. COI management is quite difficult when done with manual processes. If you simply have people fill out forms and then you store those forms in a filing cabinet, you'll never be able to follow up on those issues effectively. And if you have dozens of people listing hundreds of COIs, it becomes very difficult, if not impossible, to monitor conflicts.

The risks are high for COI mismanagement. If your company collects COI data but never follows up, that could be used against the company should the enforcement community ever investigate a potential problem. Furthermore, as companies continue to broaden their COI rules and push disclosure requirements deeper into the enterprise, the number of participants and the risk of mishandling a COI increase.

In terms of organizational culture, the COI process can be delicate. People who must share potential COIs can become defensive. If the company isn't efficient in addressing COIs, you could exacerbate employees' sensitivity to the COI process.

Conflicts of Interest Management: A Best Practices Checklist

Your organization’s COI management is strong if it includes:

□ Clear, board-approved COI policies

□ Disclosure surveys that are comprehensive, appropriate to different audiences and easy to understand

□ A process for regular information collection and a formal structure for objective review

□ Training materials and executive communications

□ “Smart forms” that make COI disclosures easier to submit. Look for automatically adjusting questions and pre-filled answer fields based on past responses

□ A central COI repository

□ An automated review process, with automated flagging and reminders to keep things moving and tracking to make sure actions happen in a timely fashion

□ An audit trail, which electronic COI solutions should generate automatically

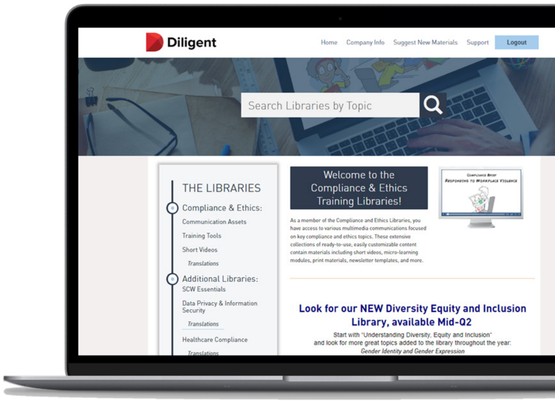
□ An independent audit at a fixed interval, say every three years

□ A dashboard summary of compliance metrics, ideally with interactive visualizations and customizable, real-time reports

□ Data analytics for understanding employee behavior and improving policies, procedures and internal controls

□ Stringent data security and data privacy with multiple layers of physical and logical protection: encryption, GDPR-ready processes, an ISO-certified hosting facility and more

3. Incident Management and Whistleblower Support



Welcome to the Compliance & Ethics Training Libraries!

As a member of the Compliance and Ethics Libraries, you have access to various multimedia communications focused on key compliance and ethics topics. These extensive collections of ready-to-use, easily customizable content contain materials including short videos, micro-learning modules, print materials, newsletter templates, and more.

Look for our NEW Diversity Equity and Inclusion Library, available Mid-Q2

Start with "Understanding Diversity, Equity and Inclusion"
and look for more great topics added to the library throughout the year:
Gender Identity and Gender Expression

Incident management is a company's ability to receive or intake an allegation about an event or action. The goal for an organization is to convey that it has heard the complaint and taken the appropriate steps to investigate and rectify any problems the company finds.

It's an increasingly high-stakes goal. Under legislation such as the Sarbanes-Oxley Act or the Dodd-Frank Act, just about every large company is required by law to have a system for internal reporting of misconduct or similar concerns. Companies are required to document their processes for incident reporting, and outside auditors can demand spot checks where they select numerous cases at random and review how those incidents were handled.

These audits and external reviews can be extensive. Auditors will want to see all the work the company has done, the supporting evidence, investigative materials, what steps were taken to remediate and so forth. And companies that don't produce those things are at risk of enforcement, with legal and financial impact, from the DOJ.

Furthermore, failure to protect whistleblowers exposes companies to litigation and enforcement risk under the Dodd-Frank Act, the False Claims Act and other statutes. Aggrieved employees can also bring civil lawsuits themselves; so even if the business ultimately prevails, corporate time, money and focus are still spent on litigation rather than on more productive tasks.

Establishing a whistleblower hotline is no longer enough. Nor are the disparate manual processes for incident management at many corporations. With tracking allegations and follow-up by spreadsheets, for example, there's great potential for error — and, more importantly, there's no way to enforce a series of repeatable steps.

Another big pitfall: lost investigations. When the institution doesn't know the status of the investigation, it can't take any mitigating steps.

Organizations need to coordinate the efforts of investigators looking into the allegation, managers who might be talking with the people who originally reported the issue and other employees taking remediation steps to fix the problem. All of this is extremely difficult to do manually, especially at large volumes.

Incident Management and Whistleblower Support: A Best Practices Checklist

Your organization's incident management and whistleblower programs are strong if you're taking a multipronged approach spanning training, reporting and incident management, with full transparency into your corporate policies and code of conduct.

This includes:

□ Broad intake capability, so people can submit allegations by email, telephone hotline, website, text messaging, a kiosk on the factory floor or even just by talking to their manager

□ Consistent protocols for incident management, with all materials from the investigation attached electronically to a single master case in an easy-to-search fashion, so you're not losing any important details

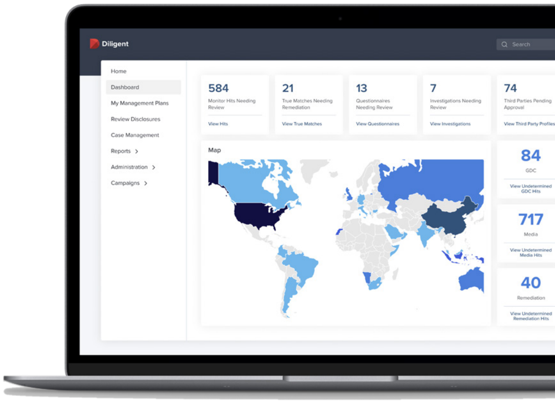
□ Scalability features like automatic task assignment, so you can effectively handle hundreds — or even thousands — of incidents at one time

□ Flexibility in areas like intake form design and customizable workflows to accommodate for twists and turns in operations

□ Case management automation to keep teams moving and free investigators to focus on the case. An automated system can also give you a full audit trail for every incident, so you'll always know what steps were or weren't taken.

□ Incident reporting that's secure, mobile-accessible, easy to operate and allows anonymous reporting for whistleblowers and sharable dashboards and reports for case managers

Compliance and Ethics Training


Diligent
Search
Home
Dashboard
My Management Plans
Review Disclosures
Case Management
Reports >
Administration >
Campaigns >
584
Monitor Hits Needing Review
View Hits
21
True Matches Needing Remediation
View True Matches
13
Questionnaires Needing Review
View Questionnaires
7
Investigations Needing Review
View Investigations
74
Third Parties Pending Approval
View Third Party Profiles
Map
84
GDC
View Undetermined GDC Hits
717
Media
View Undetermined Media Hits
40
Remediation
View Undetermined Remediation Hits

A company's compliance training covers topics that have serious ramifications for individual employees as well as the business. Yet many employees see such training as fundamentally uninteresting, irrelevant or just plain boring.

Why is this the case?

The problem starts with traditional, long-format, once-a-year training with legalistic content in antiquated formats. This has proven ineffective and elicited poor responses from employees. Compliance training materials often suffer from obscured or nonexistent takeaways. After spending 30 minutes on an e-learning training session, employees won't necessarily know what they should do in a challenging situation. Today's tech-savvy workforce sets the "effectiveness bar" even higher; gaining their attention and keeping them engaged requires video and graphics with high production values. They also expect to access your training content wherever and whenever they want it.

A significant level of "training fatigue" has settled like a pall over compliance programs. Employees may feel they are over-trained in courses that are too long and that cause interruptions in productive workflow, which can foment attitudes of resentment and resistance.

At the same time, employees may actually be under-trained due to courses that:

- ⊗ Occur too infrequently for content retention
- ⊗ Dwell in the realm of the theoretical and lack practical application to their daily activities
- ⊗ Do not include any meaningful follow up and reinforcement

To complicate matters even more, often when a specific area of risk is identified, a Band-Aid training solution may be hastily applied that is neither strategically targeted nor thoughtfully integrated within an overall compliance communication solution.

In short, organizations face many tough challenges in delivering compliance training, yet failing to engage employees could increase the risks of unethical or noncompliant behaviors.

What Effective Compliance Training Looks Like

Effective compliance training provides guidance not only on what not to do, but also on what to do. It gets right to the substance of the matter, presenting a common situation and the steps a person should take if/when they encounter it.

One example is training that blends education about company priorities and regulatory concerns ("don't bribe government officials," "assess the security of third-party tech service providers") with the policies and procedures the company uses to pursue operational goals.

Merely training employees on what a regulatory risk is and telling them the risk should be avoided fails to instruct them on how to avoid it. "Risk-based training" also appreciates that the challenge can sometimes be a serious regulatory issue (data security, for example) or a powerful group of people (senior executives able to override controls). Then training is tailored to the gravity of the risk: more extensive coursework, in-person sessions rather than online videos, and so forth.

But this is only one part of the solution. To tackle employee resistance and increase employee engagement, organizations need to incorporate behavior change and "microlearning" into their compliance training.

Microlearning is used for targeted instructional design that engages your learners, improves their retention and, most importantly, drives them to change their behavior patterns. Even when long-form training is necessary for deeper topics, such as bribery or fair competition rules, microlearning reminder tools can support the message.

In short, using behavior science and microlearning in compliance training means presenting engaging content that employees actually look forward to seeing, using strategic and frequent communications to reinforce this content, and incorporating tools for all learning styles, from short videos to microlearning modules, case studies and cartoon strips.

Best Practices for Incorporating Behavior Science and Microlearning Into Your Training Program

□ Deliver training through experiences that last no more than from 30 seconds to three or four minutes, which can easily be incorporated into the workday

□ Present interesting multimedia content with scenarios that make abstract compliance issues more concrete and relatable

□ Anticipate a variety of learning styles: visual, auditory, reader/writer and kinesthetic

□ Optimize training to match attention spans, lapses and spikes

□ Prevent cognitive overload through presenting one learning objective per lesson

□ Combat knowledge decay, which begins immediately after training, with frequent reinforcement via videos, infographics, memes, intranet blog posts and newsletter articles

□ Track participation

In Conclusion

As the regulatory landscape evolves and scrutiny intensifies, technology solutions can help compliance departments keep up, even amid constrained resources and funding, by streamlining and strengthening policy and COI management, expanding incident response and whistleblower support, and using behavior science to deliver more engaging training.

Take the next step forward for your internal compliance program.
Schedule a meeting with Diligent today.

Diligent

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com

For more information or to request a demo:
Email: info@dligent.com • Visit: diligent.com

Diligent

Technology and Risk Management: A Checklist for Successfully Managing IT Risk and Third-Party Risk

Introduction

As organizations expand their IT footprints, they become more vulnerable to cyberthreats and therefore business risk. Just one well-placed cyberattack can result in data or software damage, breaches of customer information, theft of intellectual property and business interruptions, with the damage rippling out into their supply chain, impacting on compliance with regulators, corporate reputation and revenue streams.

Third parties complicate the risk landscape even further. When organizations trust their facilities, networks and/or data to outside suppliers and partners, they open themselves up to potentially devastating financial, reputational, regulatory, operational and strategic consequences.

What happens if a hacker breaches a SaaS partner's or cloud vendor's systems — and compromises the organization's customer data? Responsibility for risk management falls on the organization. IT and risk teams can never assume that a third party is taking the necessary steps to mitigate threats.

In short, as threats to internal and external IT assets intensify, organizations must stay ahead of these risks, with a strategic plan for risk identification, mitigation, remediation and recovery.

The Challenges of IT and Third-Party Risk

Chief information security officers (CISOs), chief information officers (CIOs), IT leaders, and compliance and risk management teams face a number of challenges in minimizing their organization's IT and third-party risk exposure.

"How can we see out company's risk posture acrosss so many moving parts?"

Risk across internal IT assets and third parties is like a mosaic. Organizations need every tile to grasp the big picture, and they also need to see how the pieces fit together to form a greater whole.

Unfortunately, risk management today too often happens through a siloed approach. Information on IT assets, systems and data comes from disparate business departments and third-party vendors rather than through a centralized platform.

This means that organizations lack the aggregated view they need. Threat indicators and red flags fall through the cracks, and teams are unable to communicate and take action in real time.

"How do we know that the data we're using is up-to-date, reliable and accurate?"

Spreadsheets are ultimately tracking mechanisms, and as such, they fall short of the requirements of today's risk management and compliance teams in many ways.

For starters, spreadsheets aren't equipped to store all types of risk data, such as email conversations. Furthermore, they're difficult to collaborate across and need to be manually updated or re-created to show ongoing progress. They lack security and are easy to manipulate — whether deliberately or accidentally. Finally, spreadsheets — and the risk indicators contained within them — are easy to put into a folder and overlook, making the organization more vulnerable.

"How can we keep up with new risks as they develop?"

The elements in a company's risk profile are always changing, thanks to additions and shifts in internal IT resources, larger and more complex third-party contracts, evolving regulations and more.

A risk program needs to be able to adapt and grow in tandem with these changes, with the ability to add new assets, vendors, contracts and compliance requirements on the fly and streamline complexities along the way. While larger companies with more mature risk management programs are better equipped to tackle these challenges efficiently, siloed systems and static spreadsheets hold organizations of all sizes back in the quest to scale.

"How can we bring all the pieces together and communicate risk in a way that everyone understands?"

IT and risk management leaders presenting to the board, such as CISOs and CIOs, need to deliver an easily digestible summary of risks and opportunities, presented in a way that resonates.

Yet organizations are often held back by poor visibility and poor reporting. For consolidating information, teams often struggle to bring data together across spreadsheets and silos. When it's time to develop a report, their systems don't easily allow them to present the information in a manner that's up-to-date, intuitive and understandable.

"We just don't have the time or the budget for all of this."

Collecting data from multiple departments, vendors and outside agencies. Navigating and reconciling multiple spreadsheets. Updating PowerPoints and reports again and again as new information comes in. All this manual labor takes time — and diverts skilled IT and risk management teams away from more strategic, value-added work.

As organizations grapple with these challenges, technology can help. Specifically, solutions exist that offer a centralized and scalable environment, automated workflows and processes, third-party risk management capabilities, and robust visibility and reporting.

The following Risk Management Checklist explores these four areas in greater detail.

A Vicious Circle of Escalating Vulnerabilities

As the growing complexities of IT and third-party risk management strain internal resources, organizations need to find a solution to the problem as soon as possible.

Inadequately staffed and resourced risk management teams put an organization in an even greater state of vulnerability. Vendor service interruptions, ISP failures and data loss may signal greater business interruption, for example, and shared log-in credentials may be red flags that customers' personally identifiable information is exposed. Organizations miss these indicators at their peril.

Furthermore, an incident like a data breach is not only devastating for an organization's technical team, but it can also have lasting repercussions for the entire company. GDPR breaches, anonymous data leaks and unaddressed critical incidents not only raise the prospect of significant fines, but they also put a company's reputation at risk as incidents make headlines. All of the above can have a significant impact on shareholder value.

1. A Centralized and Scalable Environment

What new servers, systems and software have IT teams added to corporate headquarters — and which ones have they retired? Do all these assets comply with the most recent cybersecurity policies, certifications, regulations and requirements?

Looking beyond IT risk management (ITRM), to third parties: Are all vendors up-to-date with their periodic assessments and reviews? Do these assessments reflect the latest compliance requirements? And how compliant and secure are these vendors' cloud providers and other outsourced partners?

To satisfactorily answer all these questions and more, risk management teams must track status, report progress and investigate incidents in a timely fashion. On a strategic level, they must build strategic alignment around the cyber risk and IT risk landscape, making sure to accommodate each department's different goals and priorities.

Unfortunately, too many risk management teams are trying to accomplish all of this across disparate systems, spreadsheets and data sources — putting their departments and organizations at even greater risk.

Enter the centralized, scalable risk management platform. Such a platform gives organizations the integration they need, presenting a single source of truth and enabling real-time communication across departments. The right solution integrates seamlessly with existing processes, systems — both internal and external — and data sources and flexibly adjusts as the organization adds IT assets, third-party vendors, assessment forms, new processes and more.

When evaluating solutions, look for:

□ The ability to merge data from different tools

□ The ability to add, remove and adjust assets as your business grows

□ The ability to customize features as the regulatory landscape evolves

□ Integration with existing systems and processes

□ A unified platform for cross-team collaboration

□ Consistency and visibility across the organization

□ Best-in-class support from leading industry professionals

2. Automated Workflows and Processes

Robust risk management in today's business environment requires both human expertise and technological support — and this is where automation comes in.

Consider all the manual labor involved in IT risk management (ITRM) and third-party risk management (TPRM): cross-referencing vulnerabilities against assets, adding new vendor requests, scheduling vendor assessments and more. Automation supplements human effort by streamlining and strengthening the process. Organizations can deploy preconfigured content with a few clicks and automate critical IT risk & compliance workflows, freeing up their highly skilled staff for more value-added work.

Risk management, compliance and IT staff on the front lines benefit from the significant savings in time and labor. Automation transforms daunting endeavors into tasks that only take minutes.

The organization overall benefits from increased accuracy, security and efficiency. Preconfigured content keeps data standardized and consistent, and automated thresholds, alerts and workflows keep processes moving along, with fewer assessments, investigations and reviews stalled or falling through the cracks.

When evaluating solutions, look for:

□ The ability to deploy preconfigured content in just a few clicks for features like vendor applications and assessments

□ The ability to leverage previous findings, so you're not reinventing the risk management wheel

□ Automation in areas such as issue management, risk reviews and other daily risk management and compliance activities that keep teams diverted from higher-level work

□ Rules-based automation, to ensure that employees or systems don't close issues before all action items are completed

□ Robotic process automation for customized questionnaires and thresholds, as well as triggers and alerts when thresholds are breached

□ Automated, end-to-end risk scoring

□ Seamless integration with threat and vulnerability feeds

□ Features that are intuitive for users across all areas of the business — no specialized training required

□ Best-in-class support from leading industry professionals

3. Third-Party Monitoring and Management

Third parties expand both the scope and complexity of risk management.

Assessments, onboarding and ongoing monitoring can be immensely labor-intensive to manage. The shift to outsourcing and the cloud often brings fourth parties into the mix. And the stakes for getting it right are higher than ever. Any time you trust your facilities, networks and/or data to a third party, you're opening up your organization to potentially devastating financial, reputational, regulatory, operational and strategic consequences.

A third-party risk management (TPRM) solution can help on all fronts. A unified platform empowers organizations to assess, manage and monitor third-party risk with ease, while reducing the risk of error and preventing data duplication. Automation makes TPRM processes, from onboarding to contract management and beyond, more streamlined and secure.

But that's not all a modern technology solution offers for taming the complexities of TPRM. Some solutions integrate information from security and financial intelligence providers, for end-to-end assessment management. Others make it easier to present information to the board, executives and other stakeholders. Visualization dashboards and reports can provide real-time visibility into third-party risk, for example, and advanced analytics can give organizations the ability to quickly identify and prioritize their riskiest third parties. It all adds up to time savings, increased accuracy, a sharper view and more streamlined decision-making.

When evaluating TPRM solutions, look for:

□ A unified platform, with a centralized inventory and data repository

□ A dashboard view, so you can see, at any time, where a vendor is in the onboarding process

□ Pre-built industry standard questionnaires (e.g., SIG Lite and CAIQ-Lite)

□ Bulk import of third-party data

□ Risk-based assessment controls

□ End-to-end third-party assessment management

□ SLA performance monitoring and contract management

□ The ability to collect, measure and monitor data against key performance indicators

□ Integration of third-party intelligence feeds such as credit ratings, IT security risk ratings, media feeds, government watch lists and public filings

□ A platform that integrates with your company's existing systems, including your ERP solution and accounting software

□ Features that enable seamless collaboration for the entire risk management team

□ Ready-to-use visualization dashboards and reports for real-time visibility

□ Best-in-class support from leading industry professionals

4. Powerful Reporting and Deep Visibility

Risk management information only realizes its full value when it's shared — and when the recipients of this information fully understand the data's context, impact and implications.

This kind of reporting and visibility is particularly important for IT and third-party risk management. Leaders, including the board, want to know new vulnerabilities and trends in the cyber landscape, the progress of risk-reduction efforts and how the organization's security posture compares against those of its peers. Being able to provide such visibility is essential to both managing risk across the organization and building trust with the executive team.

Yet preparing risk reports has typically been a convoluted, often ad-hoc process — especially for teams tracking everything in a spreadsheet.

Fortunately, tools are available that help. These ready-to-use visualizations and executive dashboards distill data into an easy-to-understand format, communicating risk to a board that doesn't want complex technical details and enabling low-effort, data-driven decision-making.

When evaluating solutions, look for:

□ A user-friendly interface that presents data in an easy-to-understand format

□ A wide range of ready-to-go reporting and visualization options, sharable with anyone who has internet access

□ Storyboards that let you visually represent data in real time and add context

□ Integration with threat and vulnerability feeds

□ A wide range of data connectors and custom APIs for additional (and quick) information retrieval

□ Connections to risk scores and assessments

□ In-depth data analytics

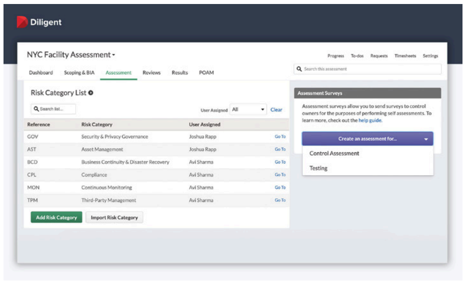
□ Advanced risk modeling for specific use cases and scenarios

□ An alert system for elevated risk and action items

□ Best-in-class support from leading industry professionals

How Diligent Can Help

When it comes to managing risk today, governance technology is the way forward. Organizations should seek a solution that not only covers all aspects of modern risk but is flexible enough to evolve as both the business and the risk landscape around it continue to change and grow.

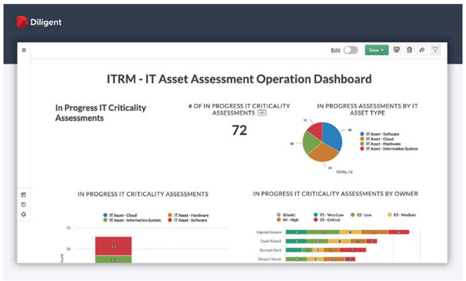


Risk Category List

Reference	Risk Category	User Assigned	
GOV	Security & Privacy Governance	Joshua Rapp	Go To
AST	Asset Management	Joshua Rapp	Go To
BCD	Business Continuity & Disaster Recovery	Avi Sharma	Go To
CPL	Compliance	Avi Sharma	Go To
MON	Continuous Monitoring	Avi Sharma	Go To
TPM	Third-Party Management	Avi Sharma	Go To

Assessment Surveys

Assessment surveys allow you to send surveys to control owners for the purposes of performing self assessments. To learn more, check out the help guide.

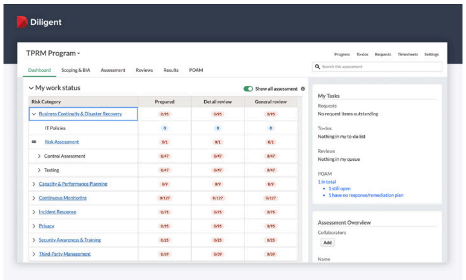

Diligent
Edit
Save
ITRM - IT Asset Assessment Operation Dashboard
In Progress IT Criticality Assessments
# OF IN PROGRESS IT CRITICALITY ASSESSMENTS
KPI
72
IN PROGRESS ASSESSMENTS BY IT ASSET TYPE
11
24
15
22
TOTAL: 72
IT Asset - Software
IT Asset - Cloud
IT Asset - Hardware
IT Asset - Information System
IN PROGRESS IT CRITICALITY ASSESSMENTS
IT Asset - Cloud
IT Asset - Hardware
IT Asset - Information System
IT Asset - Software
75
50
Count
23
IN PROGRESS IT CRITICALITY ASSESSMENTS BY OWNER
(blank)
01 - Very Low
02 - Low
03 - Medium
04 - High
05 - Critical
Vignesh Selvam
David Riddell
Basimah Syed
Deepak Nayak

IT Risk Management (ITRM) from Diligent offers:

☑ Proactive, effective and robust IT risk and compliance management

☑ A centralized and scalable cloud-based platform

☑ A foundational pillar for a proactive, truly integrated governance, risk and compliance (GRC) program — across the entire company



My work status

Risk Category	Prepared	Detail review	General review
Business Continuity & Disaster Recovery	0/95	0/95	0/95
IT Policies	0	0	0
Risk Assessment	0/1	0/1	0/1
Control Assessment	0/47	0/47	0/47
Testing	0/47	0/47	0/47
Capacity & Performance Planning	0/9	0/9	0/9
Continuous Monitoring	0/127	0/127	0/127
Incident Response	0/75	0/75	0/75
Privacy	0/95	0/95	0/95
Security Awareness & Training	0/25	0/25	0/25
Third-Party Management	0/39	0/39	0/39

My Tasks

Requests
No request items outstanding

To-dos
Nothing in my to-do list

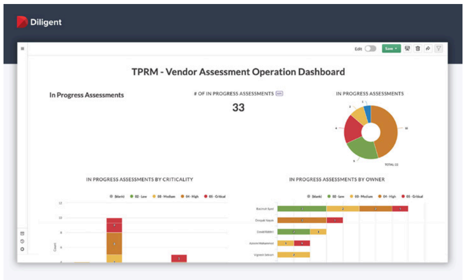
Reviews
Nothing in my queue

POAM
1 in total
- 1 still open
- 1 have no response/remediation plan

Assessment Overview

Collaborators

Name



Third-Party Risk Management (TPRM) from Diligent empowers companies to:

☑ Simplify, manage and scale an existing third-party risk-management program

☑ Establish a solid foundation to create and grow a third-party risk program — whatever the organization's size

☑ Accommodate change and third-party program maturation over time as the business, regulatory and risk landscape evolves

To learn more about how Diligent can enhance your IT Risk Management and Third-Party Risk Management programs, schedule a meeting today.

Diligent

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com.

For more information or to request a demo:

Email: **info@dligent.com** • Visit: **diligent.com**

Diligent

Modernizing Your Internal Audit Infrastructure: A Checklist for Optimizing Efficiency and Impact

Introduction

Running an internal audit department today isn't easy. Regulations and business requirements are constantly evolving. Responsibilities are expanding, with senior leadership increasingly asking for a comprehensive view of audit status and organizational risk. Traditional tools and processes — disparate documents, spreadsheets and manual workflows — struggle to keep up, posing a variety of risks and administrative challenges.

The problems start with fragmentation. Audit processes, data sources, plans, issues and remediations are too often siloed. This precludes organization-wide visibility and effective reporting. It also hinders consistency across departments; information trapped inside electronic documents and spreadsheets effectively becomes "dark data," impossible to search, reference, analyze, export, report on or access on mobile devices.

Systems are too often static and unable to keep up with evolving risks in areas such as cybersecurity or sustainability, unable to quickly adapt to changing regulations and requirements, and unable to scale as the organization and its responsibilities grow. Teams spend their time toggling across spreadsheets and ticking boxes rather than on higher-value work.

This all adds up to an untenable situation in today's business environment. Increasingly, leadership expects internal audit teams to not only identify issues and track remediations but also provide strategic insight into risk, revenue opportunities and more. It's an escalated and expanded role that often comes without a commensurate increase in budget or staffing.

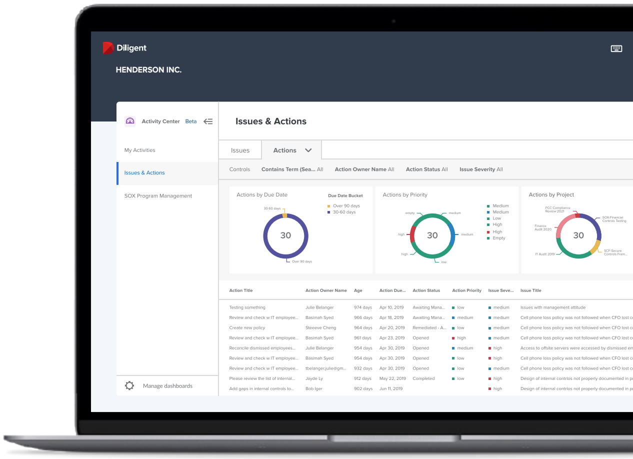
Technology is key to success and critical to keeping pace. Yet adopting a modern audit infrastructure often requires a shift in perspective.

Read on for four key steps to also building an optimized audit infrastructure, with checklists to guide your journey.

1. Centralization

Standardization, speed and simplicity — these are the benefits unified audit management platforms and centralized repositories and libraries deliver. With such centralization, audit teams can stay organized, process audits faster, reduce their workloads and aggregate assurance across the organization's overall risk and control framework, to rapidly highlight areas of concern.

A unified "source of truth" also keeps teams on the same page, for greater accuracy, less duplication and fewer repetitive tasks.



Action Title	Action Owner Name	Age	Action Due...	Action Status	Action Priority	Issue Seve...	Issue Title
Testing something	Julie Belanger	974 days	Apr 10, 2019	Awaiting Mana...	low	medium	Issues with management attitude
Review and check w IT employee...	Basimah Syed	966 days	Apr 18, 2019	Awaiting Mana...	medium	medium	Cell phone loss policy was not followed when CFO lost c
Create new policy	Steeeve Cheng	964 days	Apr 20, 2019	Remediated - A...	low	medium	Cell phone loss policy was not followed when CFO lost c
Review and check w IT employee...	Basimah Syed	961 days	Apr 23, 2019	Opened	high	medium	Cell phone loss policy was not followed when CFO lost c
Reconcile dismissed employees...	Julie Belanger	954 days	Apr 30, 2019	Opened	medium	high	Access to offsite servers were accessed by dismissed em
Review and check w IT employee...	Basimah Syed	954 days	Apr 30, 2019	Opened	low	high	Cell phone loss policy was not followed when CFO lost c
Review and check w IT employee...	tbelanger.julie@gm...	932 days	Apr 30, 2019	Opened	low	medium	Cell phone loss policy was not followed when CFO lost c
Please review the list of internal...	Jayde Ly	912 days	May 22, 2019	Completed	low	high	Design of internal contrlos not properly documented in p
Add gaps in internal controls to...	Bob Iger	902 days	Jun 11, 2019			high	Design of internal contrlos not properly documented in p

Audit infrastructure built on a centralized platform can:

□ Store test results, supporting documentation and evidence, all in one place

□ Plan, conduct fieldwork, execute on procedures, identify findings and make recommendations from a single platform

□ Manage all the audit programs from a central location

□ Maintain a library of past audits, workflow templates, customized workpapers, and risk and control matrices

□ Integrate audit analytics and questionnaires

□ Mass migrate legacy or multi-department issues into a single, secure platform

2. Automation

Centralized platforms are one step to improving audit efficiency. Automation is another, with several other benefits — such as scalability.

With automated workflows based on industry best practices, teams can conduct more audits in less time and free up their days for strategic insight. When programs are preconfigured, teams can stay up to date on and respond quickly to evolving audit standards and regulations, without cumbersome manual research or having to move between numerous programs and systems. Additionally, with mobile capabilities, auditors can conduct tasks at any stage of the process at any time, from any device.

Automation also enables internal audit teams to swiftly scale their operations, adding new processes, requirements, workflows and staff at the speed of change.

Automation as part of a technology-based audit infrastructure should include:

☐ Standardized templates and reusable risk and control libraries

☐ Automatically deployable and trackable audit questionnaires, with the ability to easily capture evidence, and make in-line citations

☐ Automated workflows to manage requests and responses from control owners across the organizations

☐ The ability to quickly plan, schedule and assign audit plans and manage them through to completions

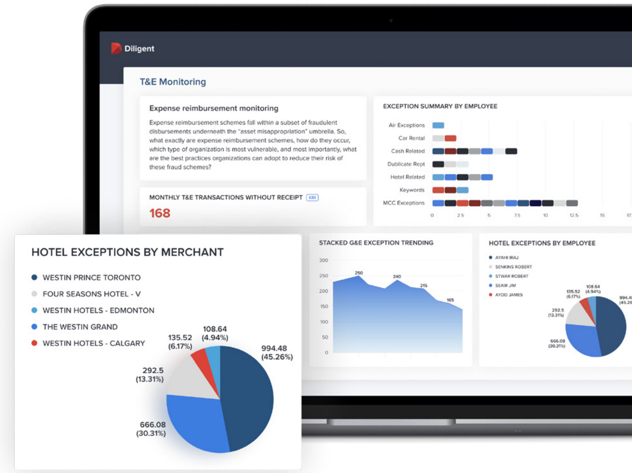
☐ IIA-recommended methodology and best practices built into programs and processes

3. Visibility

Across these processes, systems and data sources, internal audit teams need to be able to see what's going on, both for their own objective oversight and to guide leadership in critical business decisions.

How is the audit program performing? What are the biggest risks that could derail business strategy?

Here's where audit dashboards and reporting tools come in. Such technology distills the complexities and delivers real-time insights for informed decision-making. The best solutions also provide assurance, with data that is defensible to regulators and external auditors during investigations.



Expense reimbursement monitoring

Expense reimbursement schemes fall within a subset of fraudulent disbursements underneath the "asset misappropriation" umbrella. So, what exactly are expense reimbursement schemes, how do they occur, which type of organization is most vulnerable, and most importantly, what are the best practices organizations can adopt to reduce their risk of these fraud schemes?

Modern audit dashboards and reporting tools enable teams to:

- ☐ Gain real-time visibility into individual audits and overall strategy and communicate progress
- ☐ Zero in on the highest priority risks via drilldowns into status, findings, audit logs and more
- ☐ Perform real-time risk assessments
- ☐ Illustrate how audits tie to strategic objectives and key areas of risk
- ☐ Be confident that the information they're using is up-to-date, consistent, accurate and aligned with the latest regulations and requirements

4. Continuous Assurance

As audit teams are all too aware, identifying issues is just one part of the job. Teams must also monitor progress and remediation — activities currently rife with inefficient manual processes.

Consider all of the operational processes that require continuous oversight: SOX, P2P, SoD, payroll, the list goes on. Modern audit technology serves as an accelerator and force multiplier for performance and risk monitoring, automatically testing controls, delivering continuous assurance and freeing up auditors for more strategic work.

Look for the ability to:

□ Track and automate real-time KPIs/KRIs

□ Automatically test controls against standards and regulations and monitor them in real time

□ Track, remediate and report on deficiencies, issues and findings

□ Automate action plans and assignments for follow up, with the ability to cite evidence directly within the platform

□ Analyze transactional data in real time for leakage

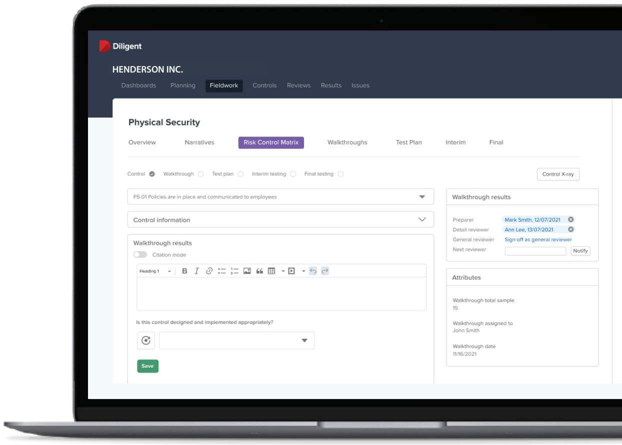
□ Enable collaboration, escalation and reporting on issues and deficiencies

Diligent for Audit Management

Diligent Audit Management helps audit teams move forward with the four key steps of centralization, automation, visibility, ongoing assurance:

- ☑ A unified platform with centralized data, templates and libraries
- ☑ Automation and dynamic workflows supported by agile, best-in-class audit methodology
- ☑ Built-in analytics and machine learning capabilities
- ☑ Real-time dashboards and one-click reports

But this is just the beginning. For audit teams tasked with doing more with less, while evolving into an expanded role, Diligent provides:



Physical Security

Control ● Walkthrough ○ Test plan ○ Interim testing ○ Final testing ○

PS-01 Policies are in place and communicated to employees

Control information

Walkthrough results

Citation mode

Is this control designed and implemented appropriately?

Walkthrough results

Preparer: Mark Smith, 12/07/2021

Detail reviewer: Ann Lee, 13/07/2021

General reviewer: Sign-off as general reviewer

Next reviewer:

Attributes

Walkthrough total sample
15

Walkthrough assigned to
John Smith

Walkthrough date
11/16/2021

Effortless and Efficient Audit Management

With Diligent, audit teams are able to effortlessly and efficiently manage every audit. They can conduct more audits in less time with automated workflows grounded in best-in-class audit methodology, which simplify the end-to-end audit life cycle.

Diligent connects directly to any data source with built-in data connectors, including SAP, Oracle and Concur. This removes work duplication and the risk of human error and gives teams the ability to analyze 100% of their data. Automated monitoring of operational control processes — such as P2P, SoD, payroll, general ledger analysis, AP analysis, fixed asset management, access control, SOX and AML — saves time and resources that are typically spent on manual monitoring.

Diligent further helps teams work more efficiently through the ability to schedule and manage audit projects and the ability to maintain a library of past audits, workflow templates, and risk and control matrices. Working from a single source of truth both eliminates repetitive tasks and duplication and enables the audit program to scale. Moreover, with Diligent's mobile apps and offline modes, audit teams can conduct fieldwork, including end-to-end audits, from anywhere and on any device.

Strategic Insight

Diligent Audit Management empowers audit teams to turn audit into a strategic advantage. Teams are able to maximize executive visibility into audit workflows and insights with one-click reports that keep stakeholders informed and individualized dashboards that drill down into audit status, findings and remediation plans.

Real-time dashboards and reports both support agile decision-making and instill executive confidence in the audit program. For external communications and investigations, audit teams are able to report on the performance of their entire program with data that is defensible to regulators and external auditors.

Continuous Assurance

Finally, Diligent Audit Management enables audit teams to operate as a strategic audit leader that mitigate risks in real time, supporting their ability to swiftly identify areas of concern, focus on the highest priorities and ensure remediation.

With Diligent Audit Management, teams are able to:

☑ Create risk-based audit plans that span the entire audit universe and aggregate risk assurance across the company's enterprise risk management framework

☑ Track and automate performance and risk KPIs/KRIs in real time

☑ Track remediation efforts by owner with scheduled follow-ups, reminders, and notifications

☑ Directly map audit engagements to strategic business priorities

☑ Use machine learning and analytics to perform advanced analyses and predict future trends

Take the next step in modernizing your audit infrastructure. Download Diligent's Audit Management Software Buyer's Guide.

Diligent

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com.

For more information or to request a demo:
Email: **info@dligent.com** • Visit: **diligent.com**

Diligent

Governance Checklist: A Guide to Keeping Up With Rising Stakeholder Demands

Companies today face more scrutiny than ever before. A growing network of stakeholders is demanding transparency and accountability on issues that go beyond the bottom line.

Increasingly, an organization's purpose and societal impact will play an important role in driving a company's valuation, public perception and overall growth and performance.

Challenges

The rising demands of stakeholder capitalism require greater vigilance and foresight than ever before. To summarize these challenges, today's organizations face:

Increased demands for transparency and accountability from all stakeholder groups

Lack of standard reporting frameworks, metrics or investor alignment on critical issues like ESG, DE&I and climate

Lack of visibility into peer group data, benchmarking and disclosures

Enhanced levels of cyber risk brought on through new virtual working models

Poor visibility into organizational risk posture (operations, reputation, cyber, etc.)

Legacy technology systems, which lack the integrations required to meet future disclosure obligations

An increasingly competitive labor marketing demanding enhanced oversight from boards and leadership

Shifting the Governance Roadmap

As stakeholder demands rise, companies may need to rethink their governance infrastructures (i.e., process, technology, skills) to accommodate new expectations and regulations. This guide outlines the four steps needed to build a modern governance infrastructure.

1. Establish an Intelligence Framework

2. Integrate Data & Reporting

3. Secure All Board & Executuve Communications

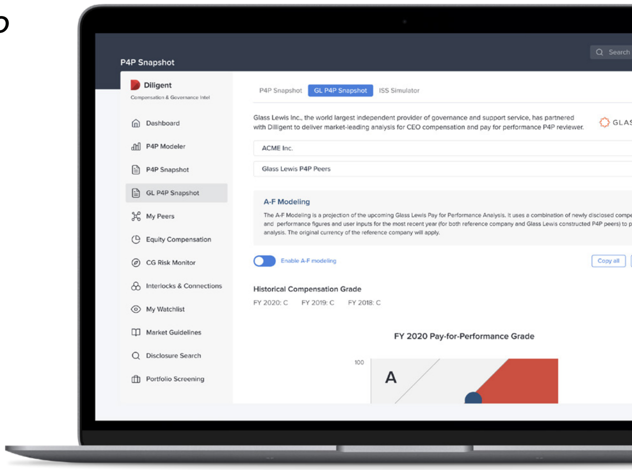
4. Drive Board Performance

1. Establish an Intelligence Framework

Access and curate the information your organization needs to remain vigilant on stakeholder sentiment.

Organizations that don't have a constant pulse on the stakeholder landscape may find themselves blindsided by shareholder proposals, proxy advisor recommendations or say-on-pay votes. With a holistic, real-time view of stakeholder sentiment and peer benchmarking, your organization will be better equipped to engage with investors and mitigate shareholder activists.

With the right technology in place, today's general counsels and corporate secretaries have the power to enhance visibility across the organization by curating the information that matters most.



Glass Lewis Inc., the world largest independent provider of governance and support service, has partnered with Diligent to deliver market-leading analysis for CEO compensation and pay for performance P4P reviewer.

ACME Inc.

Glass Lewis P4P Peers

A-F Modeling

The A-F Modeling is a projection of the upcoming Glass Lewis Pay for Performance Analysis. It uses a combination of newly disclosed compe and performance figures and user inputs for the most recent year (for both reference company and Glass Lewis constructed P4P peers) to p analysis. The original currency of the reference company will apply.

Enable A-F modeling

Historical Compensation Grade

FY 2020: C FY 2019: C FY 2018: C

FY 2020 Pay-for-Performance Grade

Required Capabilities

- □ Monitor competitors and industry landscape
- □ Monitor the evolving regulatory landscape, globally and locally
- □ Monitor stakeholder sentiment and reputation
- □ Curate important news and articles for board members and executives
- □ Model various peer groups based on investor and proxy advisor parameters
- □ Search and compare proxy disclosures (e.g., climate, diversity) across thousands of companies
- □ Benchmark against peers on ESG standards, executive pay and other governance metrics
- □ Model and evaluate pay-for-performance plans and measure compensation according to relevant performance metrics

Ask About These Diligent Capabilties

- **Media and regulatory monitoring**
- **Peer group modeling and benchmarking**
- **Disclosure search tool**
- **Exclusive access to Glass Lewis data, modeling and methodology**
- **Pay-for-performance analysis**

2. Integrate Data & Reporting

Navigate and prepare for upcoming regulations and stakeholder expectations.

Forthcoming regulations around ESG and data privacy will require organizations to meet complex reporting requirements in the months ahead. However, few companies are prepared for this lift from a data and technology perspective. In a November 2021 survey by Censuswide, respondents who lacked confidence in their risk and compliance capabilities cited three common barriers: (a) difficulties providing real-time reporting, (b) legacy systems that create silos, and (c) ineffective methods of illustrating or interpreting data.

Platforms that leverage robotic process automation are effective at gathering information across disparate systems and data sources (whether internal or external) so that organizations can meet the myriad reporting obligations ahead.

Required Capabilities

- ☐ Gather, prepare and analyze data across legacy systems
- ☐ Integrate external data sources and benchmarking
- ☐ Compare organizational data against regulatory standards and frameworks (e.g., TCFD, GDPR)
- ☐ Monitor internal operations according to risk thresholds
- ☐ Power dashboards and visualizations for the board and executive team
- ☐ Provide assurance for ESG programs and public-facing commitments

Ask About These Diligent Capabilties

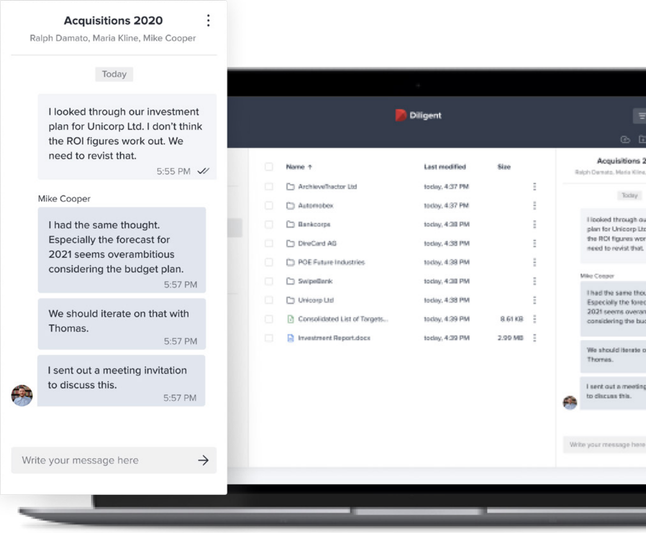
- **ESG data solutions**
- **Risk management integrations**
- **Subsidiary management capabilities**

3. Secure All Board & Executive Communications

Maintain a secure line of sight into confidential channels while minimizing risk.

In a virtual, work-from-home world, the risk of cyber breaches has skyrocketed, and so have the implications. Following a cyber breach, significant business consequences ensue including loss of valuable IP, loss of consumer trust, reputational damage, fines and negative press – just to name a few.

Boards and executives remain the most attractive targets, yet few organizations have sealed off communications on encrypted channels. A comprehensive governance program mitigates information leaks, enables easy collection of critical information from board members and executives, and ensures a dedicated communication channel in crisis times.



Acquisitions 2020

Ralph Damato, Maria Kline, Mike Cooper

Today

I looked through our investment plan for Unicorp Ltd. I don't think the ROI figures work out. We need to revist that. 5:55 PM

Mike Cooper

I had the same thought. Especially the forecast for 2021 seems overambitious considering the budget plan. 5:57 PM

We should iterate on that with Thomas. 5:57 PM

I sent out a meeting invitation to discuss this. 5:57 PM

Write your message here

Name ↑	Last modified	Size
ArchieveTractor Ltd	today, 4:37 PM	
Automobex	today, 4:37 PM	
Bankcorps	today, 4:38 PM	
DineCard AG	today, 4:38 PM	
POE Future Industries	today, 4:38 PM	
SwipeBank	today, 4:38 PM	
Unicorp Ltd	today, 4:38 PM	
Consolidated List of Targets...	today, 4:39 PM	8.61 KB
Investment Report.docx	today, 4:39 PM	2.99 MB

Required Capabilities

- ☐ Leverage one secure platform to manage all sensitive board and executive materials (e.g., board books, meeting minutes, financials)
- ☐ Securely share virtual meeting links
- ☐ Protect peer-to-peer communication between board members or executives
- ☐ Securely share documents with trusted third parties (e.g., auditors, consultants, outside counsel)
- ☐ Enable the ability to remotely wipe data on devices that are lost or stolen
- ☐ Establish advanced settings for privacy shielding, user permissions and data storage
- ☐ Establish a secure, dedicated channel for crisis communications
- ☐ Establish virtual data rooms for special projects or M&A transactions

Ask About These Diligent Capabilties

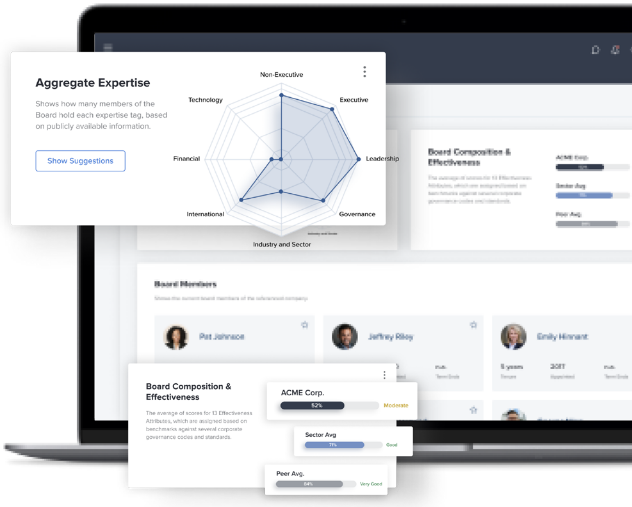
- Board meeting management
- Virtual meeting capabilities
- Secure peer-to-peer messaging
- Secure meeting workflows

4. Drive Board Performance

Cultivate an engaged board and leverage directors' strengths effectively.

To future-proof the organization for the challenges ahead, board performance and composition are key. Board members and their skill sets must be diverse in ways that mirror the organization's long-term strategy and equip the organization to address evolving stakeholder demands. Optimizing board processes also plays an important role in shifting the time and energy from administrative processes to more strategic outputs.

When a board is functioning at its best, diversity becomes a mindset, not a finish line; evaluations are regarded as opportunities for improvement rather than a check-the-box exercise; and board processes are streamlined wherever possible.



Aggregate Expertise

Shows how many members of the Board hold each expertise tag, based on publicly available information.

Board Composition & Effectiveness

The average of scores for 13 Effectiveness Attributes, which are assigned based on benchmarks against several corporate governance codes and standards.

Required Capabilities

□ Collect and analyze board evaluations within your board management software

□ Establish a process for virtual signatures and minutes approvals

□ Curate important action items onto a board member homepage

□ Access a vast database of board candidates based on advanced search criteria

□ Access a large network of diverse and rising candidates based on desired criteria

□ Tap into a rich library of governance research and thought leadership

Ask About These Diligent Capabilties

- **Board homepage & notifications**
- **Board candidate database**
- **Automated D&O questionnaires**
- **Research, events, thought leadership**
- **DocuSign integration**

See Diligent in Action

Learn why over 1 million users from across 25,000 organizations trust Diligent solutions for governance, risk, audit, compliance and ESG. Schedule a meeting with a Diligent advisor.

SCHEDULE A MEETING

Diligent

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com

For more information or to request a demo:

Email: **info@dligent.com** • Visit: **diligent.com**