MITRATECH | GRC

Regulations without borders: The importance of TPRM and extended enterprise risk management as your global network grows

Risk is no longer bound to your headquarters. Keep you and your vendors compliant with regulations in every region where you operate.

It feels like a new regulation comes out every day — and the scope of these regulations has also grown as our networks have. Businesses went from on-site server rooms to third-parties, cloud providers, etc, **but outsourcing services does not outsource the risk.**

As your network grows, you are responsible for ensuring your vendors, partners, and other third parties are complying with your internal policies and procedures. And to add yet another layer of complexity, you'll need to make sure you are complying with every regulation that impacts a region where you have a certain number of employees.

Did you know?

As of 2021, if you have an operation in Germany with 3,000 employees or more, you now need to comply with **The German Supply Chain Act**.

In January 2024, that scope will be reduced to 1,000 employees. Failure to comply can reportedly reach €800,000 (Ecommerce Germany).

3,000+ Employees

> "It's no longer important where your headquarters are, but where you operate your business."
>
> - Claudia Howe, Executive Director of GRC Solutions at Mitratech

It's one thing to achieve, monitor, and report on compliance within your organization, but to achieve that success on a larger scale, you'll require better visibility and control across your full value chain. Some call this vendor risk, extended enterprise risk, third-party risk management, etc.

Ask the experts:

What does it mean to **"do extended enterprise"** well?

- Create a tiering process to categorize vendors according to their risk potential (a vendor that deals with proprietary or sensitive data on a daily basis, for example, would be considered high risk).
- Have the appropriate controls in place for each vendor based on where they fall within the tiering process.
- Define a cadence for that vendor relationship – for high-risk vendors (like an ATM provider, for example), there should be a close relationship where you catch up regularly.

Bonus Tip: Always think of a "retirement plan" - what do you do if someone can no longer serve as a partner? **It's not about being pessimistic. It's about being prepared.**

Want to learn more? Catch Mitratech's Morning Coffee Show episode on global & extended regulatory environments.

Watch Now

So, what do organizations need to keep an eye on heading into 2024?

With regulatory compliance more interconnected and extended across borders than ever before, there are three risk categories to keep an eye out for in 2024.

1. CYBER THREATS

September 2023 saw a year-high of 3.8 MILLION compromised records, bringing the year's total to 4.5 BILLION. (IT Governance, 2023).

Digital transformation is one of the key driving factors of cyber breaches and attacks. As businesses grow on a global scale and engage with more and more third party vendors, the risk for cyber threats increases astronomically.

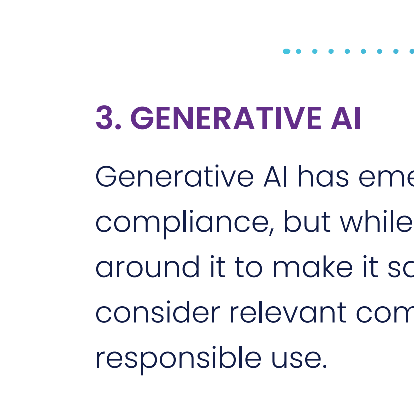
The percentage of data shared with third parties will ramp up over the next five years from 30% to 41% by 2026. (Forrester, 2021).

While larger organizations used to be the primary targets of bad actors seeking to steal sensitive customer information, they've shifted their tactics, and third-party cyber attacks are now becoming more prevalent.

82% of third-party threats present a significant risk for organizations. (Forrester, 2021).

The best way to keep your organization safe in the face of cyber threats is to have a robust third-party risk management program in place to guarantee employee and partner compliance, regardless of where they are located.

2. ESG



TPRM also has the ability to assist global businesses with complying to increasingly important ESG strategies. The research shows that more countries are requiring companies to disclose their ESG performance in one format or another.

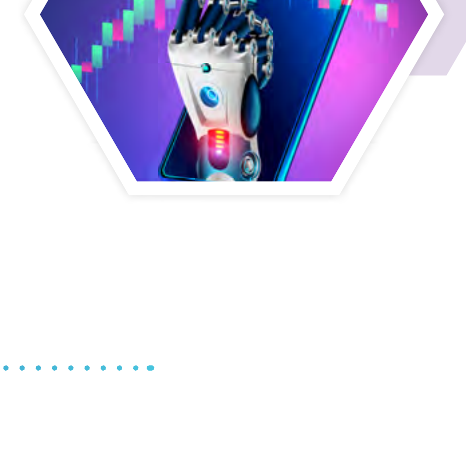
The number of ESG reporting provisions issued by governmental bodies has **grown 74%** over the last four years. Today there are nearly **400 reporting provisions in the 80 countries** (Carrots and Sticks, 2023). On a global scale, it is imperative that businesses mitigate risk by complying with all provisions not only where the headquarters are, but of all countries where the business, and their third-party partners, are operating.

ESG strategies can affect operating profits by **as much as 60%**, if done compliantly (McKinsey, 2023).

3. GENERATIVE AI

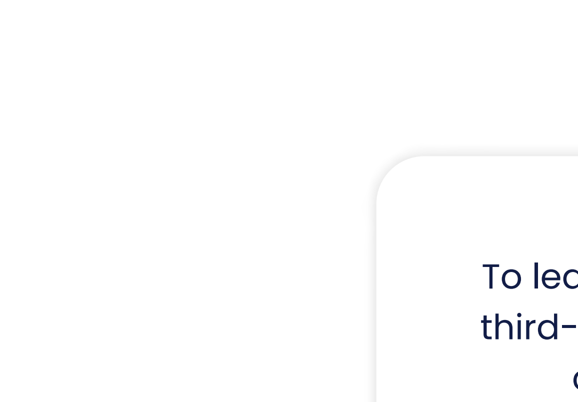
Generative AI has emerged as a new tool to help businesses with compliance, but while it holds great potential, it will require a framework around it to make it safe. Like ESG regulations, organizations must consider relevant compliance standards to ensure safe and responsible use.

34% of companies currently use AI, a number that is continuously growing while an additional 42% explore AI. (IBM, 2022)



5 best practices for generative AI compliance:

1. Follow standards of responsible data handling and storage
2. Always explain the origin and limitations of generated content
3. Thoroughly evaluate generative AI providers
4. Conduct regular risk assessments and audits
5. Educate users and stakeholders



Managing risk without borders

As regulations continue to shift and your employee or vendor networks expands, so does the scope of your compliance responsibilities. You now need to consider:

- Am I compliant with all of the regulations where I do business, not just where I am headquartered?
- Which related parties do I need to extend these internal policies and procedures to in order to ensure they're compliant as well?

To learn more about how integrating a third-party risk management program can benefit your company -

Visit www.Mitratech.com