5x5 series: Insights and actions

How can an organization monitor its electronic communications for risk concerns and proactively alert its legal, compliance, risk management and other relevant teams if it finds indications of a potential problem? A frequent response has been, “Not easily.” Traditional automated techniques for monitoring electronic communications can trigger alerts that turn out to be inaccurate or incomplete. Moreover, following up on these alerts in a meaningful way is often an ad-hoc, labor-intensive exercise.

Recent advances in technology can assist organizations in finding indications of possible financial crime and misconduct in their electronic communications stream. The result is that organizations across a range of industries are taking a fresh look at ways to monitor their electronic communications for early signs of wrongdoing. Below, are five insights into

---

5 insights you should know

Electronic communications monitoring plays a crucial role. Public scrutiny is on the rise, with a greater emphasis on the personal accountability of executives. As the volume of electronic communications increases, manual review of such communications can be inefficient and even ineffective.

Effective solutions can make the difference. Effectively tracking electronic communications is more than a focus on meeting regulators’ expectations. A monitoring solution that flags potential issues may mean the difference between containment and crisis.

It may be less expensive to manage electronic communications data consistently. Dealing with misconduct after the fact consumes a lot of time and resources, as groups such as compliance, investigation, and internal audit typically become involved.

It’s worth the effort to future-proof. Monitoring technologies have been around for a while, but they often rely on techniques that are prone to false positives and may provide partial coverage; that limited ability comes under stress as data types and volumes increase.

There’s no one-size-fits-all solution. Modern e-communications monitoring tools are highly nuanced and complex. Few are plug-and-play. Customization is required to address different situations, standards, and data sources.

---

5 actions to take now

Embrace sophisticated analytics. Regulators are using analytics to look for patterns of potential violations. Develop advanced capabilities for capturing and analyzing data, aimed at reducing the incidence of false positives. Prioritize and focus review workflows using machine learning models.

Invest in effectiveness. Create a centralized function—dedicated from the business—dedicated to review, disposition, and escalation. Effective, independent monitoring has the potential to catch small problems before they turn into big ones.

Focus on consistency. Establish consistent, continuous monitoring of electronic communications systems to provide management the ability to focus on real risks sooner, and the confidence to limit overly broad and inefficient monitoring approaches.

Adopt innovative solutions. Address challenges proactively, adapt amid disruption, and keep pace with expectations. Remember that advanced technology solutions still take time and effort to enable. Arrive at a selection as thoughtfully as possible with emerging requirements in mind.

Consider nuances. Address and embrace nuances of linguistics and communications metadata to move from reviewing a stream of false positive search results to gaining control over your e-communications compliance process.

---

Connect with us

Bart Siegel
Managing Director
Deloitte Transactions and Business Analytics LLP