Guidepost

ADDRESS YOUR COMPLIANCE "TAIL RISKS" NOW

Now is the time to shore up your compliance risk management programs. Otherwise, the likelihood and severity of violations and enforcement could increase significantly. Just last week, Acting U.S. Comptroller of the Currency Michael Hsu, rightly warned of the need to strengthen your risk management programs due to the Russia / Ukraine war and other "tail risks," which are defined as unlikely but highly impactful risk events. Tail risks have often included geopolitical risk, cyber risk, inflation and rate risk, asset price risk, and recession risk. Acting Comptroller Hsu pointed out that not only have the likelihoods for each tail risk increased, but different tail risk events may be linked and materialize simultaneously. He stated that these tail risks warrant "*greater caution and risk management vigilance … perhaps more than any time in recent memory*."

Acting Comptroller Hsu's warning is particularly timely in view of the multiple risks unfolding currently, including the continuing and potentially expanding Russia – Ukraine war; heightened / emboldened cybercrimes, and other geo-political and economic storm clouds ahead made up of global inflation, supply chain shortages, and overall stress in the markets.

Acting Comptroller Hsu, in coordination with his European and global regulatory counterparts, underscored the need to refresh enterprise risk management processes, stress testing under new and emerging scenarios.

In this regard, don't forget your **compliance** and **ethics risks**. And keep in mind that these tail risks and the need for urgency to upgrade your compliance and ethics risk management program extends across ALL industries, not just financial services.

For example:

1. Increased cyber-attacks threaten your clients', company's, and employees' confidential data. This can happen at any time and across multiple industries and geographies.
    1. A breach against your company or even one of your competitors can prompt a chain reaction of payments,

governance, and media inquiries, and an operational and communications nightmare.

2. Are your cyber desk-top exercises really "fit-for-the-ever-changing-purpose" world?
3. Have you refreshed not only your business impact analyses and risk assessments, but also extended it to anticipate and address collateral consequences from a compliance risk perspective?

2. Your growing crypto trading and banking business might lead to unknowing OFAC, EU or other regulatory sanctions evasion, according to the Office of the Comptroller of the Currency and *The Wall Street Journal* . Have you refreshed, let alone, created a crypto compliance risk assessment?

3. Do you really know your UBOs (ultimate beneficial owners) – especially if IP addresses are hacked or manipulated?
    1. Don't be surprised if enemy states or agents of such are moving their ownership interests into non-sanctioned countries, entities, or shell companies.
    2. If you are a correspondent bank, or a respondent bank with other banks as your clients, do you really know your customers' customers' customers?
    3. Are your payments filtering truly working in a timely and refreshed manner?
    4. What is your "bench strength" to always keep your operations and compliance teams ready, like having 2-3 lines of a fast-moving ice hockey team / game. The ice these days is quite slippery!

Therefore, **DO THE FOLLOWING**:

1. Refresh your compliance risk assessments and controls
    1. If they are annual – consider monthly or at least quarterly, targeted updates to validate that your documented inherent risks, control effectiveness

and especially residual risks have not hit "red" into the high and trending higher risk categories.

2. Have your teams on call to parachute into operationally risky businesses and regions to prevent and detect violations of law and regulation – beyond sanctions and especially around misconduct against consumers, markets, and communities.

2. Re-look and refresh your overall KYC, surveillance, and sanctions compliance programs – are they really working? In my previous blog, "Is Your Russia-Ukraine and Overall Sanctions Compliance Program Really Working? (Don't Find Out the Hard Way)", I outline how you and your company should be benchmarking and adapting continuously against leading- and expected compliance practices.

3. Don't put all your resources into one region – "read across" your other regions, products, clients and think ahead for emerging risks
    1. Know your regulators – work and dialogue with them to demonstrate your due diligence to refresh your compliance and ethics risk management program across your organization.
    2. Demonstrate that these tail risks can lull management into a false sense of security – but will your firm withstand a false sense of cyber- and financial crime security?

4. Keep your CEO and your board informed of your firm's increased compliance and ethics residual risks — because **your inherent risks have certainly increased, including tail risks.**
    1. What was low last year might be inherently high this year.
    2. Your controls of yesterday, therefore might not be effective any longer.
    3. Has your "enforcement risk" grown exponentially because you have not refreshed your compliance risk management program?
    4. Have you stress tested your controls to see if they will be effective if different

tail risk events are linked and materialize simultaneously?

These are just a sample of open questions to consider. If you can't answer these questions, then take action to get the answers. If you don't have the bandwidth to conduct frequent compliance risk assessments, engage an outside expert to help. In the long run, completing these tasks and reviews now can help you keep from running afoul of regulations and the potential for costly fines.

ERIC YOUNG

Senior Managing Director

Eric T. Young advises highly regulated organizations on reengineering compliance, ethics, and regulatory technology programs to enable reputable and sustainable business growth. He has deep regulatory experience having spent close to 40 years in chief compliance officer roles at some of the world's largest institutions, including five global banks. Throughout his career, Mr. Young has remediated and transformed corporate compliance programs and financial crime compliance programs including sanctions; integrated compliance and ethics cultures between regions, countries and companies to ensure consistency across enterprises; built compliance budgets; enhanced reporting; created governance frameworks and risk assessment, monitoring and testing programs; closed compliance gaps; restructured compliance teams; and mentored junior staff to create a pipeline of future compliance leaders and enable grassroots compliance ideas, solutions and digital upgrades.