

Global Economic Crime Survey 2024

Report on Ukraine



About this document



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. One should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Advisory LLC, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of anyone acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Should you have any questions regarding this publication, please contact Andriy Tretyak, Forensic Leader at PwC Ukraine, andriy.tretyak@pwc.com.

Table of contents

1	Global highlights	4
2	Key findings in Ukraine	5
3	Section 1. Corruption	6
4	Section 2. Procurement fraud	10
5	Section 3. Export Controls and Sanctions	14
6	Section 4. Supply Chain	20
7	Key contacts	24



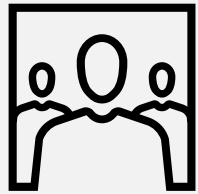
Global highlights

In today's global and interconnected environment economic crime is a pervasive challenge. Thus proper and timely response to this issue is crucial for securing organizations' performance, assets and viability.

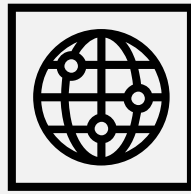
The risk of economic crime is more complex than ever before — and it is far more challenging to both create value and protect it.

It is against this backdrop that the PwC Forensics practice embarked on its Global Economic Crime Survey, conducted between January and March 2024, the latest in a series of studies dating back more than 20 years.

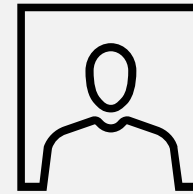
Highlights of global respondents



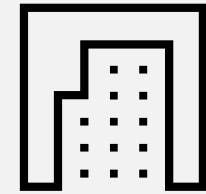
~ 2,500
respondents



63
territories



~ 33%
C-suite executives

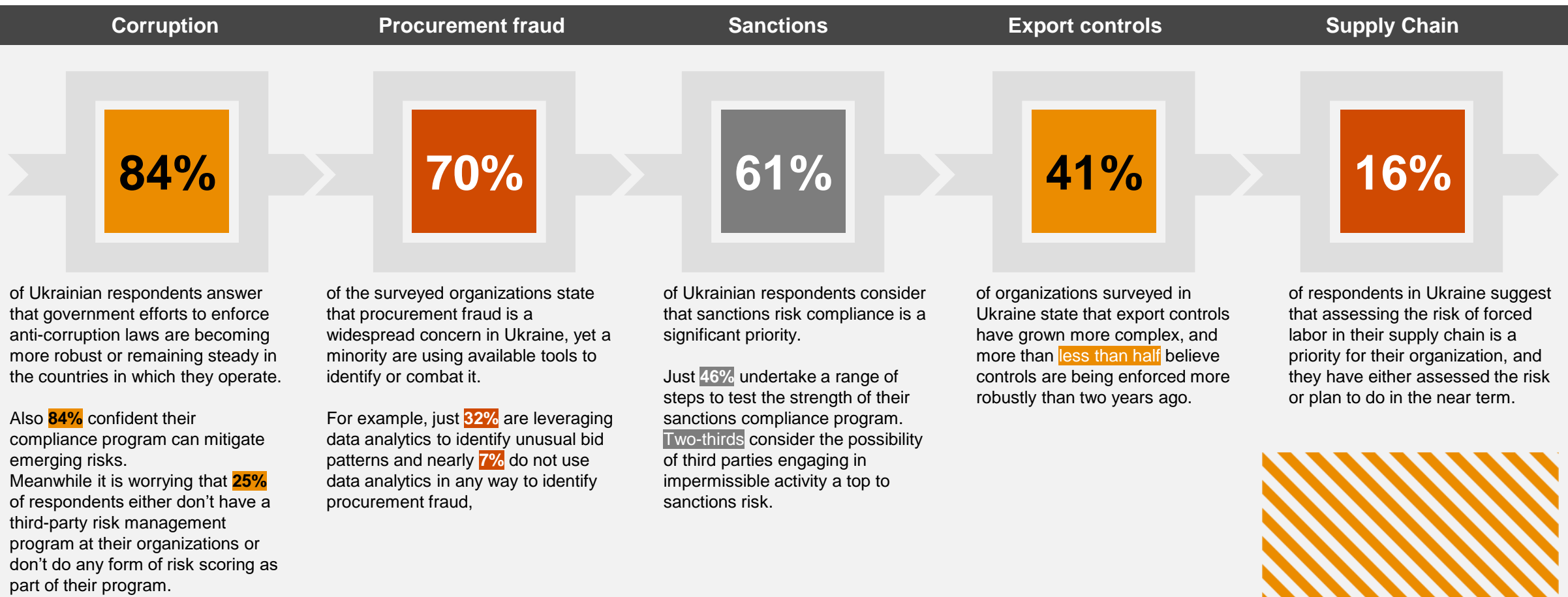


29
industries

5 key industries in Ukraine:

- Consumer products and retail
- Agriculture, forestry and fishing
- Banking and capital markets
- Financial services
- Healthcare

Key findings in Ukraine





Section 1

Corruption

Rising expectations and missed opportunities — today's challenges



Governments around the world are signaling their rising expectations that corporate compliance programs become more sophisticated.

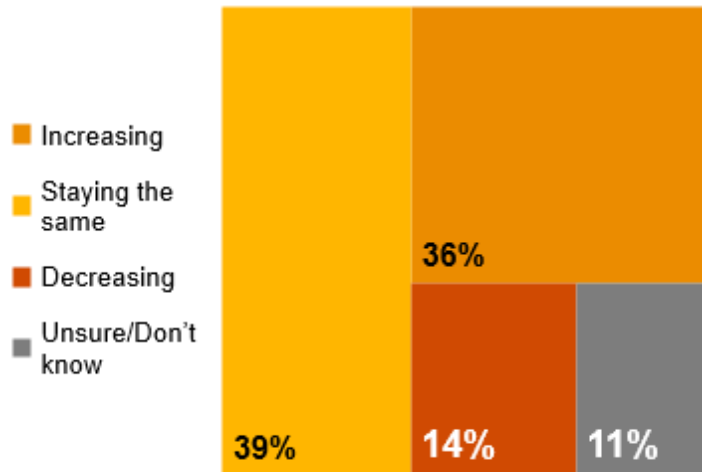
A decade after Ukraine's Revolution of Dignity and subsequent work to establish new anti-corruption and judicial sector institutions, and in the context of Russia's brutal full-scale invasion, the country faces a growing opportunity and need to advance a next generation of oversight, revenue growth, and anti-corruption reforms within a new set of key institutions for economic revitalization and good governance.

Corruption risks

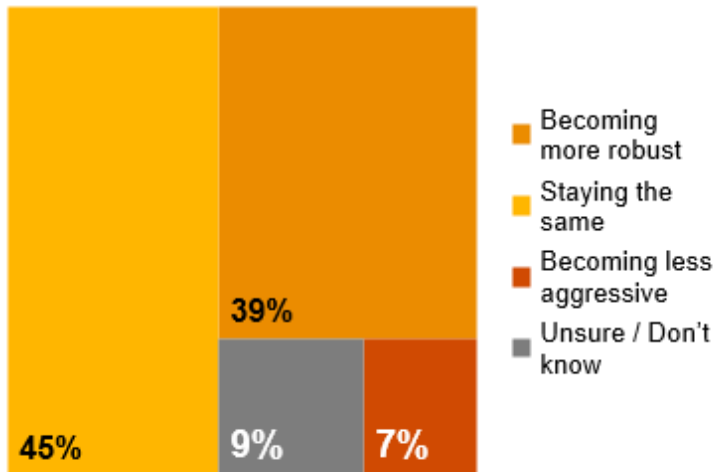
In Ukraine, **36%** of respondents state that the **corruption risks are increasing**, although the **government's efforts have become more robust** that confirmed by **39%** of answers.

Corruption risks are not receding, while enforcement efforts are gathering pace

Respondent opinion on state of corruption risk



Respondent opinion on state of anti-corruption law enforcement



Q12. In your opinion, are risks associated with corrupt or improper payments to government officials/and or commercial customers in the last 12 months?

Q14. How are government efforts to enforce anti-corruption laws changing in the last 12 months?

Respondents show confidence that their **compliance program can mitigate emerging corruption risks**. Prevailing **84%** of respondents state that they have it handled.

84%

Confident that organization's compliance program is capable of mitigating emerging corruption risks

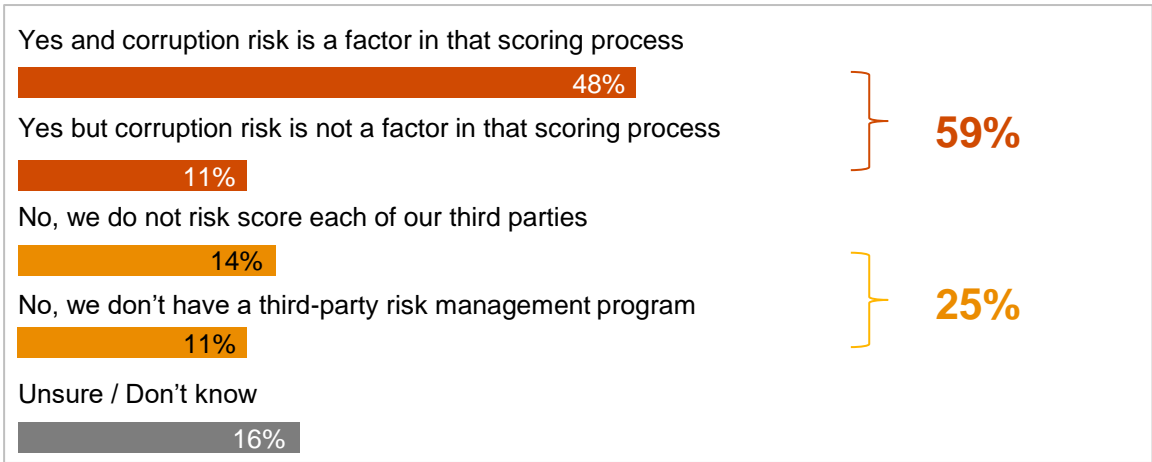
16%

Not confident

Q13. How confident are you that your organization's compliance program is capable of mitigating emerging corruption risks?

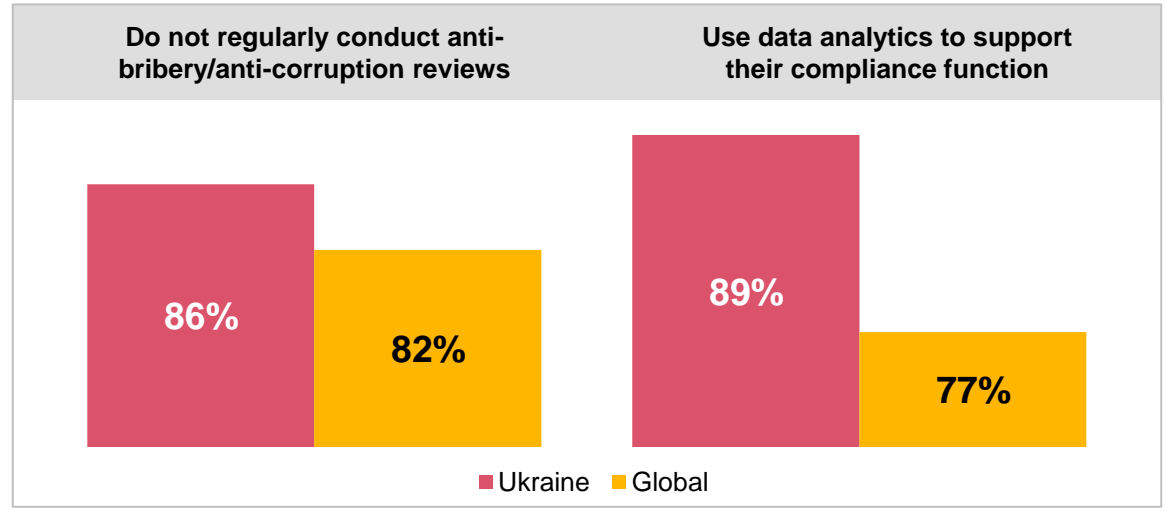
Anti-corruption compliance

- Among the components of an effective **third-party anti-corruption compliance program, risk scoring and anti-bribery/anti-corruption (ABAC) reviews** are crucial.
- More than half (**59%**) of respondents **conduct risk scoring as part of their third-party risk management**, and nearly four out of five of those consider corruption risk in that process.
- What's alarming is that **25% of the surveyed organizations either don't have a third-party risk management program at all** or, if they do, risk scoring is not done.



Q15. Does your organization assign a risk score to each of its third parties as part of its third-party risk management program?

- When it comes to **ABAC reviews of the third parties**, there is substantial room for improvement because **86% of respondents state that their organizations do not conduct such reviews regularly**.
- The use of data analytics and root cause analyses are all important elements in an effective anti-corruption compliance program. **89% of respondents are using data analytics to support their compliance function**.



Q16. Has your organization conducted an anti-bribery/anti-corruption audit at one or more of its third parties in the last two years?

Q18. How does your organization use data analytics in support of its anti-corruption compliance objectives?

Key ideas for further consideration



Undertaking periodic compliance program assessments helps benchmarking existing programs against regulatory expectations and peer best practices. Brief annual employee surveys focusing on ethics and compliance are recommended to provide useful additional data points.



Integrity due diligence of counterparties can ensure additional data for further use in cooperation with them. Using open registries and specialized databases is recommended to avoid cooperation with unreliable partners.



Identifying potential corruption risks within your organization and developing a scoring methodology that will allow assessing corruption risks and strengthen financial control.



It is worth coordinating the use of various internal and external data sources to more comprehensively assess compliance risks for each country in which the organization operates.

Procurement fraud

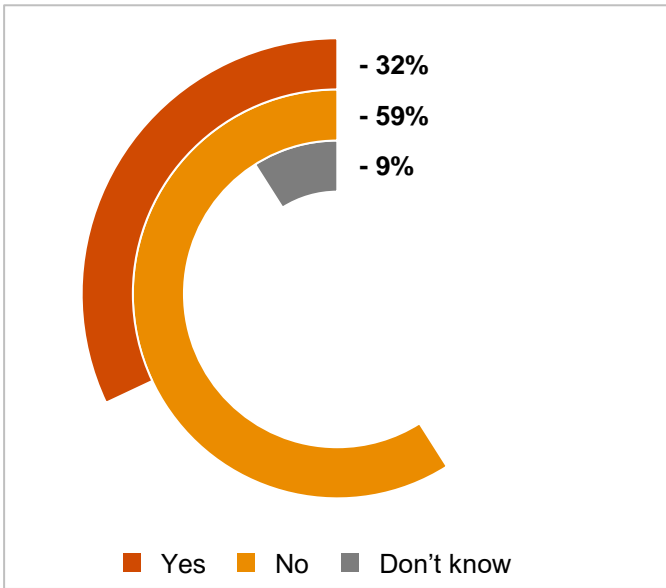
A fresh look at a persistent peril

In all of its forms, procurement fraud remains a continuing challenge.

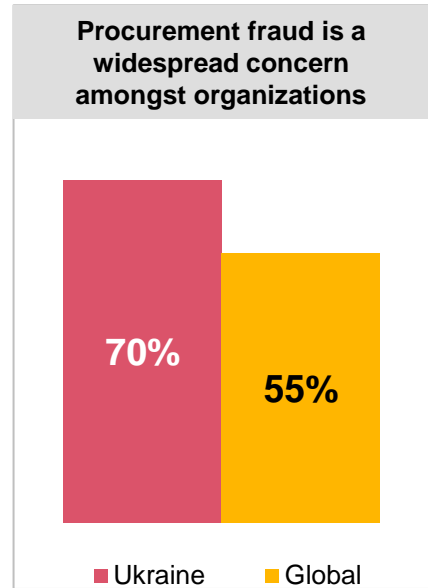
Procurement fraud erodes profitability, destroys value and undermines a positive corporate culture. Unfortunately, bad actors exist inside and outside of the organization. Insider threats are not limited to cybercrime or intellectual property theft—countering procurement fraud should be an integral element of organizations' insider threat programs.

Procurement fraud

- > This survey shows that **32% of respondents** experienced fraud, corruption or other economic / financial crime within the last 24 months.
- > **70% state that procurement fraud is a widespread concern amongst the surveyed organizations in Ukraine**, meanwhile in the world this percentage is 55%.



Q1. Has your organization experienced any fraud, corruption or other economic/financial crime in your country within the last 24 months?



Q10. Is procurement fraud a widespread concern amongst businesses?

- > In Ukraine **30% of the surveyed organizations do not take measures to identify their losses from fraud during procurement**, while others take the following steps to mitigate the risk of procurement fraud:

	Ukraine	Global
1 Revising the vendor selection process	84%	60%
2 Adopting a robust conflict of interest policy	77%	56%
3 Improving anti-fraud training for procurement personnel	75%	53%
4 Strengthening processes to confirm adequate documentation and proper authorizations	70%	71%
5 Utilizing a centralized function (e.g. compliance center of excellence) to resolve escalations of pricing discrepancies or signs of fraud or improper payments	41%	40%
6 Leveraging data analytics to identify unusual bid patterns	32%	26%

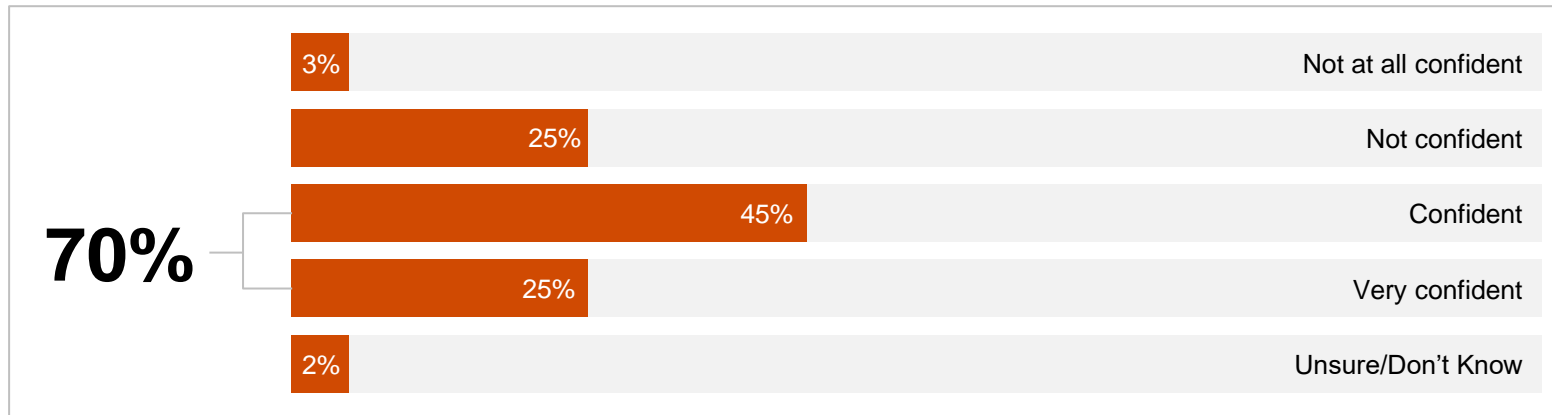
Q11. What steps, if any, is your organization taking to mitigate the risk of procurement fraud?

Third-party risk management

In order to prevent the risk of procurement fraud, 84% of respondents in Ukraine revise the vendor selection process regularly

Both in Ukraine and globally **70% of respondents** have a complete and accurate understanding of all of their third parties (vendors, suppliers, distributors, customers, etc.). And about **60% of respondents** have an organization's third-party risk management program that includes risk scoring of their third parties.

While data to support diligence efforts on third parties is often plentiful and enterprise resource planning (ERP) systems reinforce good hygiene in procure-to-pay processes, **technology isn't solely a force for good**. In the hands of fraudsters, advanced technology also enables sophisticated efforts to perpetrate procurement fraud.



Q6. How confident are you that your organization has a complete and accurate understanding of all of its third parties (vendors, suppliers, distributors, customers, etc.)?

The survey shows that in Ukraine **half of respondents have conducted an enterprise-wide fraud risk assessment** in the last 12 months, and a further 9% plan to do so within a year going forward.



Q6. Has your organization conducted an enterprise-wide fraud risk assessment in the last 12 months?

Key ideas for further consideration



Having a well-defined conflict of interest (CoI) policy as well as regular training on that policy is essential for preventing and countering procurement fraud.



An organization-wide fraud risk assessment helps identify weaknesses and develop effective measures to address them across all departments and processes.



The compliance function needs to secure buy-in from procurement on a risk-based approach to third parties, including due diligence ahead of onboarding, onsite reviews where appropriate and re-screening of legacy and high-risk vendors.



Refreshing risk assessments for the highest-risk segments and geographies and improving efforts to risk score vendors by including more varied sources of data, i.a. Artificial Intelligence (AI) and Generative AI (GenAI).



Involving individuals at mid-management levels, not just from Procurement and Supply Chain, but also from human resources, information technology security, compliance, internal audit and investigations to counter issues related to procurement fraud risk management.



Section 3


Export Controls and Sanctions

Cross-border conflicts adding to the complexity
of corporate compliance efforts



**The issue of export control and sanctions
is more acute than ever.**

Geopolitics, including the Russia–Ukraine war, tensions between China and the US, and uncertainty in the Middle East, give rise to the export controls and sanctions regulatory environment in which organizations around the world must operate.

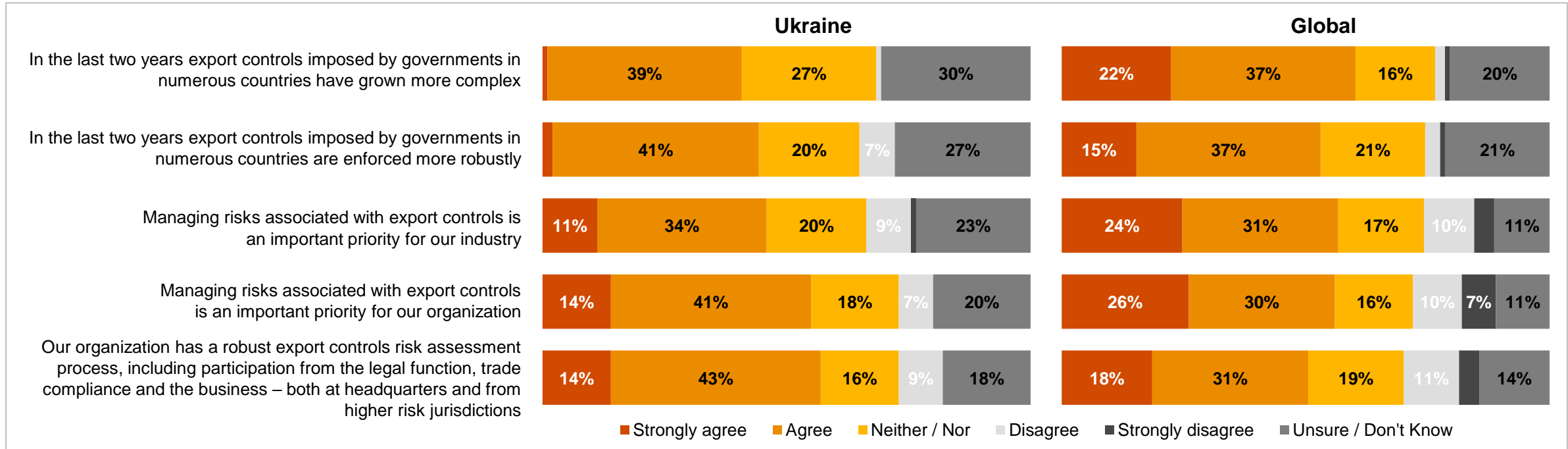


Export controls

Ukrainian respondents state that export controls have grown more complex in the last two years and at the same time the enforcement efforts have been on the rise. For example, almost half of respondents suggest that **export controls are being enforced more robustly** than two years ago.

> **45% of Ukrainian respondents answer** that managing export controls risk **is a priority for their industry** and over half of respondents state that it is crucial to their organization.

> These organizations also appear to be taking action. **More than half of respondents** state that they **have a robust export controls risk assessment process** that includes participation from Legal, Trade Compliance, and the business in both headquarters and higher-risk jurisdictions.



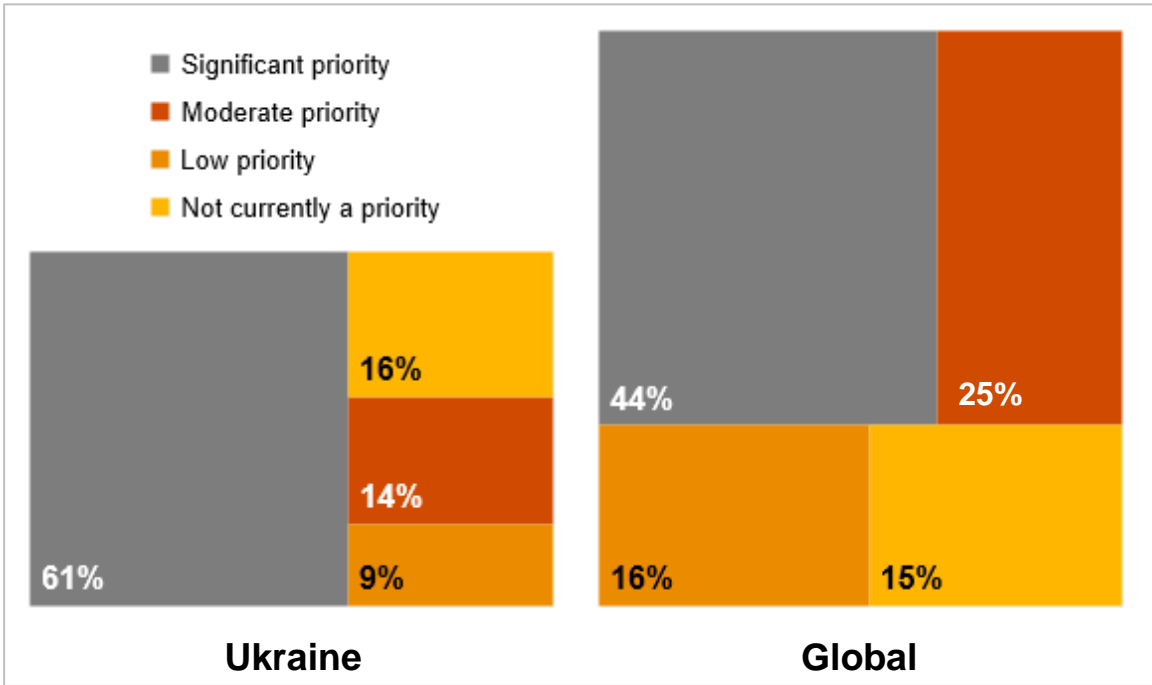
Q27. To what extent do you agree or disagree with each of the following statements?

Sanctions compliance (1/2)



Sanctions play an important role in the global fight against financial crime, terrorism or other unethical activities, which can pose threats to international peace. The main goal of sanctions compliance is to protect businesses.

> In Ukraine **61% of respondents state that consider sanctions risk compliance a significant priority for their organization** in comparison with 44% globally.



Q28. To what extent is sanctions risk compliance a priority within your organization?

> The obtained responses also clearly outline **the list of key areas which can pose the sanctions compliance risks** for organizations in Ukraine and globally.



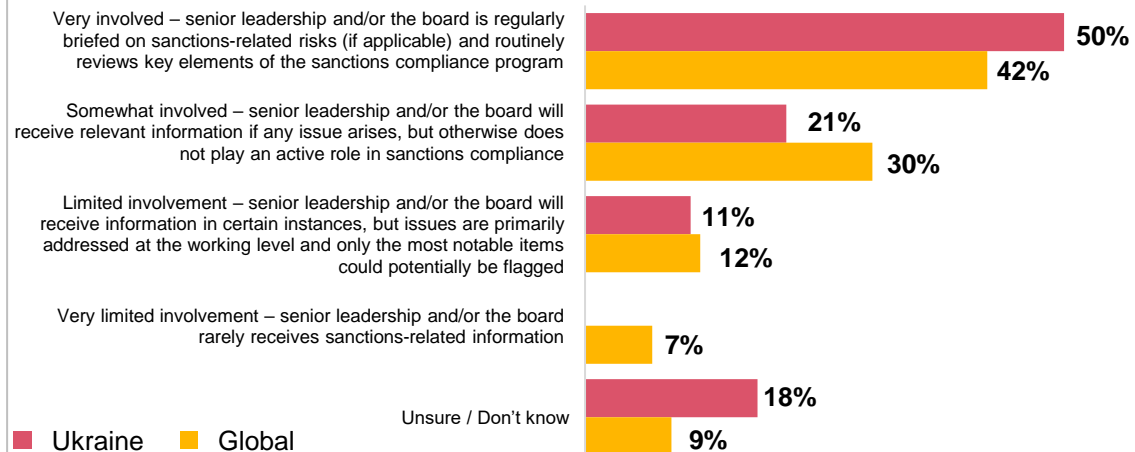
Q29. Which of the following do you think poses the greatest sanctions compliance risk for your organization?

Sanctions compliance (2/2)

According to the Ukrainian respondents, the **level of involvement of senior management and the Board of Directors** in addressing their organization's sanctions compliance risks is the following:

- **Every second** is very involved;
- **Every fifth** is somewhat involved;
- **Every tenth** has limited involvement;
- about **20% of respondents** do not know such information.

How involved in addressing your organization's sanctions compliance risks is senior management and/or the Board of Directors?

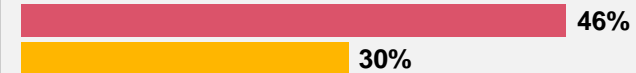


Q30. How involved in addressing your organization's sanctions compliance risks is senior management and/or the Board of Directors?

This survey shows that **Ukrainian organizations consider a more comprehensive approach to reviewing their sanctions compliance program** than globally.

Almost **half of Ukrainian respondents** consider undertaking a range of testing steps* which include reviewing policies and procedures, confirming that staff are dispositioning sanctions alerts and cases correctly via testing and/or QA/QC, and testing sanctions systems, including data lineage and system performance. While one in five Ukrainian respondents doesn't know the organization's approach to testing the strength of their sanctions compliance program (in comparison with one in ten respondents globally).

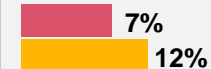
We undertake a range of testing steps*



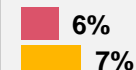
Our testing is primarily focused on reviewing policies and procedures and confirming that alerts and cases are dispositioned correctly



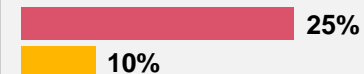
We do not regularly test our organization's sanctions compliance program, as we have assessed our sanctions risks to be low



We do not have a testing function/do not regularly test our organization's sanctions compliance program



Unsure / Don't know



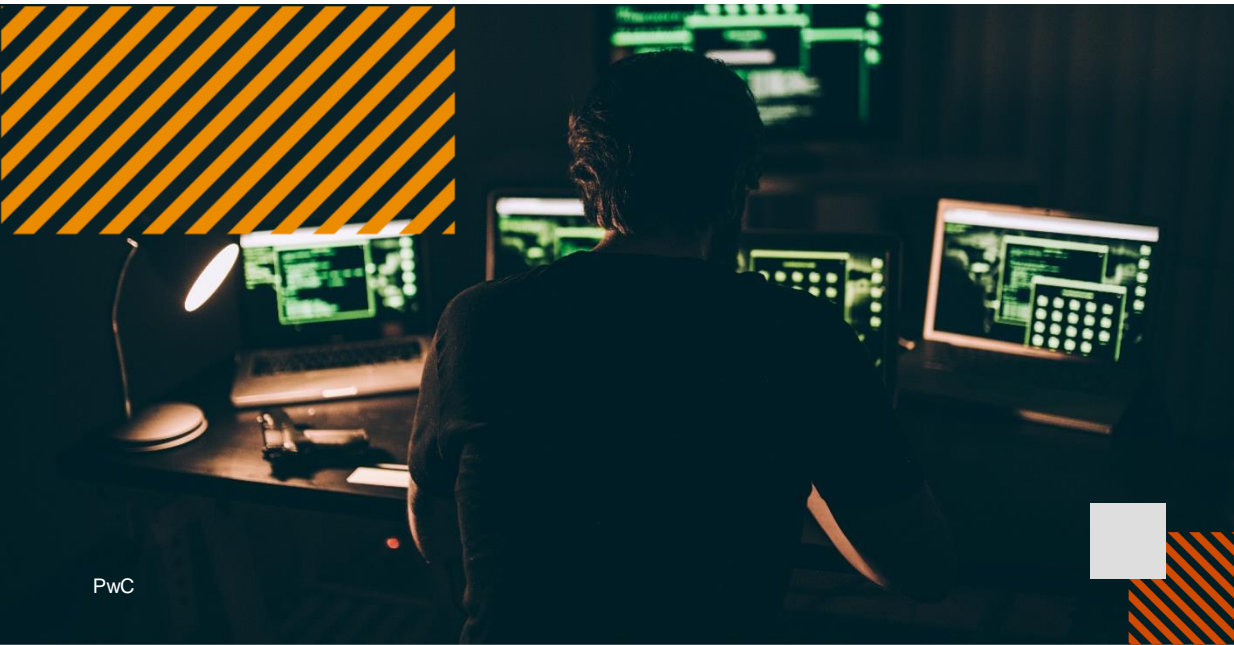
■ Ukraine ■ Global

Q31. Which of the following best describes your organization's approach to testing the strength of your sanctions compliance program?

Sanction technology

> When it comes to the possibility that new technologies, such as AI, could help considerably with sanctions compliance efficiency and effectiveness, the jury is still out. 35% of Ukrainian respondents state that **these technologies will dramatically increase the efficiencies** of sanctions program, including reducing costs.

> At the same time, **14% of respondents answer more regulatory guidance is needed for how new technologies** can become an integral part of sanctions' compliance practices.



Q32. Thinking about new technologies and systems (e.g., artificial intelligence (including machine learning) or generative AI), what impact do you think they will have on your sanctions compliance program in the next 12 months?

Key ideas for further consideration



Trade compliance violations often begin with conflicts of interest, such as receiving personal benefits from parties or individuals in sanctioned countries. Staying alert to conflicts of interest is crucial.



Monitoring social media for images of its products being used in sanctioned countries is crucial for organizations that produce physical, branded products.



Intensifying efforts to leverage sales data and identify possible instances of diversion to sanctioned countries by third parties in neighbouring countries is crucial.



Paying attention to aware of the limitations to geo-blocking, particularly with respect to sanctioned territories that exist within non-sanctioned countries (e.g., Crimea) and to efforts by individuals to use virtual private networks to defeat geo-blocking IT systems.



Section 4

Supply Chain

Protecting human rights through providing transparency in supply chains

Rising public scrutiny and rapidly evolving regulatory landscape are placing increased pressure on organizations to identify and mitigate risks associated with forced labor and other human rights abuses in their supply chains.

Complexity only continues to grow across the global economy and the resources to compensate for it are diminishing, resulting in a world in which organizations are pushed to do much more with much less.

Supply Chain outlook



To gain better understanding where the highest human rights risks lie within their supply chains, many organizations have started down the path of supply chain mapping.

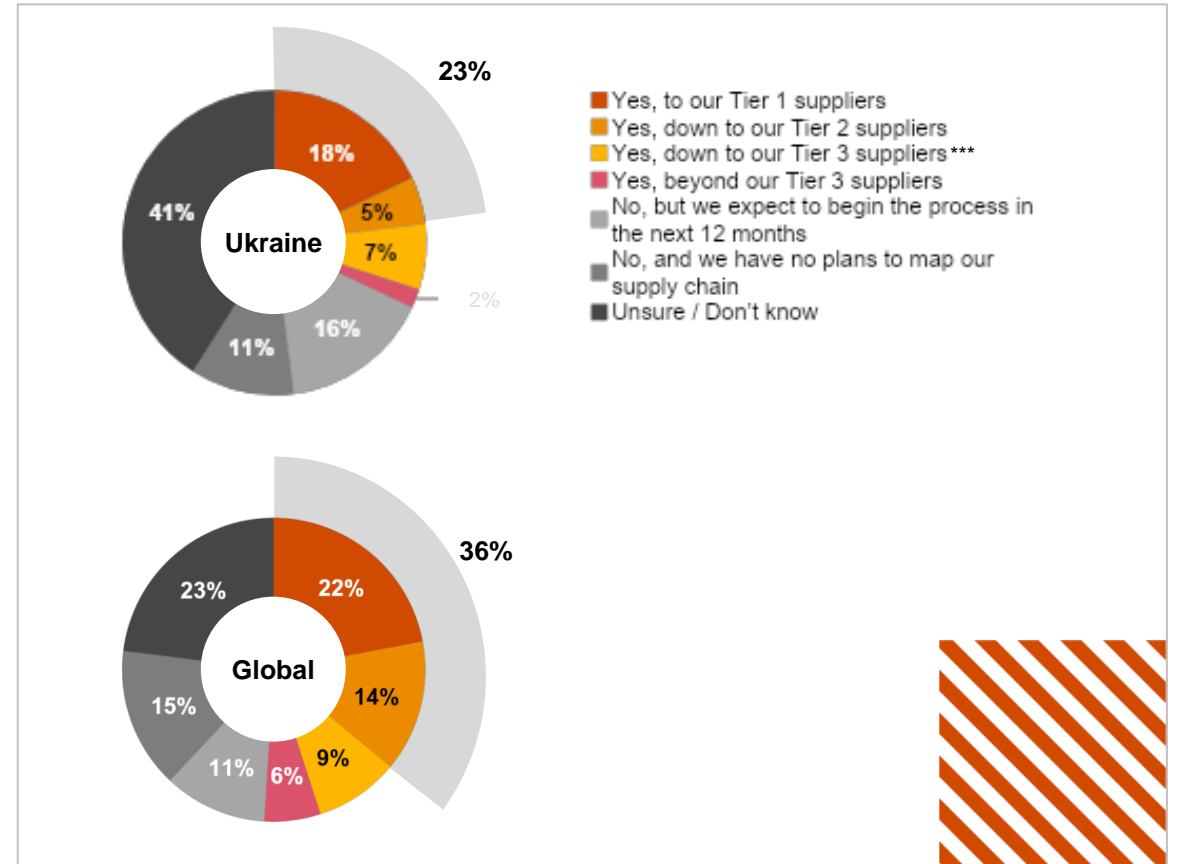


23% of Ukrainian respondents have mapped their supply chains to Tier 1* (T1) or Tier 2** (T2) suppliers unlike 36% globally.

****Tier 1 suppliers:** These are direct suppliers of the final product.

****Tier 2 suppliers:** These are suppliers or subcontractors for Tier 1 suppliers.

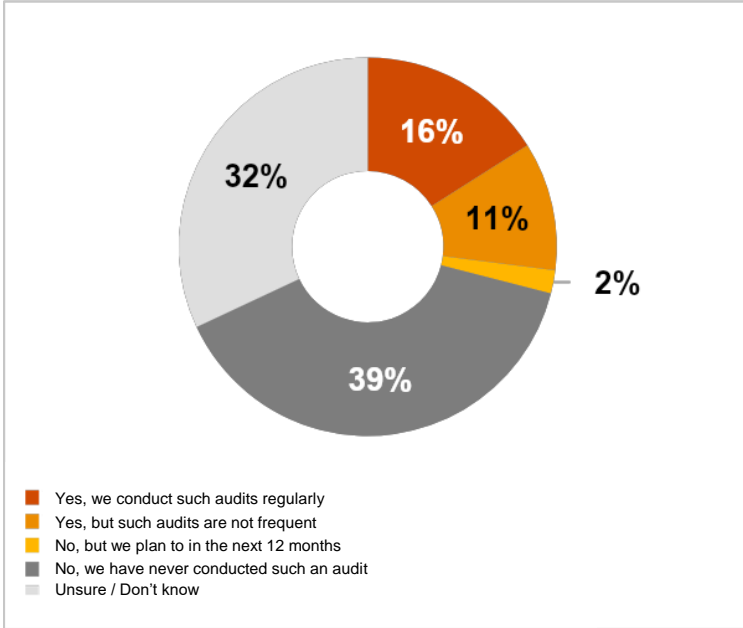
***** Tier 3 suppliers:** These are suppliers, or subcontractors for Tier 2 suppliers



Q24. Has your organization mapped its supply chain?

Forced labor

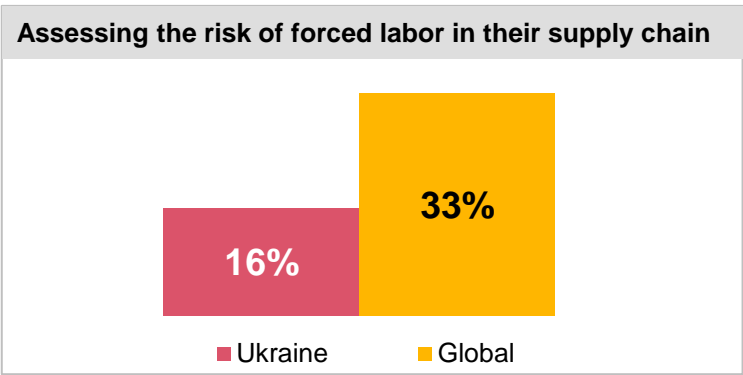
> This survey shows that **41%** of Ukrainian respondents have **never conducted due diligence** on their third parties to **assess their compliance with forced labor regulations**.



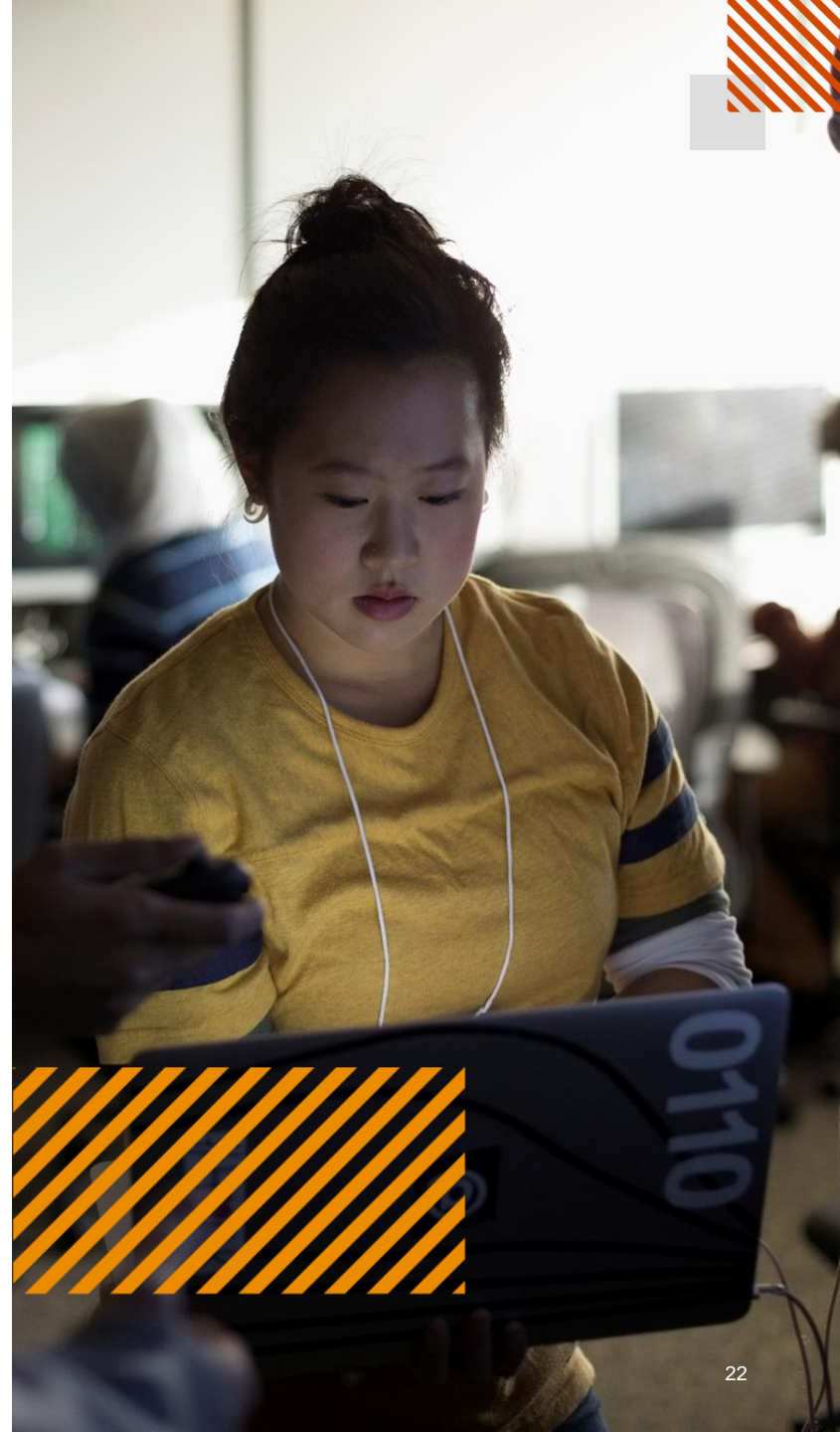
Q25. Has your organization ever conducted an audit of any of its third parties to assess its compliance with forced labor regulations?

> Forced labor is still a **burning issue and a real problem** to many countries, including Ukraine. Military hostilities, economic instability, high population mobility, labor migration, and growing unemployment may cause wider exploitation of persons and create a threat of getting into a forced labor situation.

> In Ukraine **only 16%** of respondents state that **assessing the risk of forced labor in their supply chain is a priority** for their organization.



Q22. Regardless of whether your organization is covered or not by the Corporate Sustainability Reporting Directive (CSRD), do you believe that assessing the risk of forced labor in your supply chain is a priority for your organization?



Key ideas for further consideration



Insisting on supply chain mapping as an integral part of the organization's third-party risk management program ensures comprehensive risk assessment and resilience.



It may be prudent to expand regular integrity due diligence of counterparties and include the review of their compliance with the legislation on the prohibition of the use of forced labor.



Evaluating local and foreign markets to determine whether the revenue opportunity and operational risks there warrant a supply chain strategy is crucial, i.a. covering weighing local market revenue or production facilities against existing operational risks.

Do you want to know more about how to prevent, investigate and remediate economic crimes?

Contact our subject matter experts



**Andriy
Tretyak**

CFE, CISA, Forensic Leader,
PwC Ukraine
andriy.tretyak@pwc.com



**Bogdana
Tyshchenko**

Senior Manager,
Forensic Services, PwC Ukraine
tyshchenko.bogdana@pwc.com



**Anastasiia
Myroshnychenko**

Manager,
Forensic Services, PwC Ukraine
anastasiia.myroshnychenko@pwc.com



**Liliia
Mudrak**

Associate,
Forensic Services, PwC Ukraine
liliia.mudrak@pwc.com



Thank you

[pwc.com](https://www.pwc.com)

©2024 PwC. All rights reserved.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. One should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Advisory LLC, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of anyone acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.