Leading practices for export compliance audits



Getting the nuts and bolts of a compliance audit right can be an invaluable step to wider business successes, write Amie Ahanchian, Brandon Barela and Sarah Blank.

Developing a robust audit programme can be a game-changer for corporations navigating the increasingly complex world of global trade, as an effective audit programme is clearly an integral element of any world-class export compliance programme. In this article, we set forth leading practices for executing an export compliance risk audit and explain why audits are a necessary aspect of a company's internal control framework and overall compliance life-cycle.

Compliance audits vary in type – from organisational self-assessments, corporate-level export compliance reviews, internal audits, external assessments, and government-directed audits. The scope of each audit can also vary significantly – from general regulatory assessments policy compliance, transaction-level reviews, and so forth. A well-executed audit involves planning, performing, reporting and implementing improvements based on the results. In this article, we set forth a blueprint for conducting an internal audit of a company's export compliance activity.

Thinking ahead to the results of the audit

While it is important for companies to conduct audits to evaluate regulatory compliance, assess the effectiveness of existing corporate objectives and processes, and identify and analyse risks, what is equally as important is how export compliance leaders incorporate the audit findings into their organisation's compliance life cycle. To be impactful, compliance leaders should use findings to further vet the root cause(s) of compliance errors, formulate and execute a plan for corrective action(s), and leverage the outcome of these analyses as the basis of future compliance training programmes. In other words, the audit should not be a unique event, but rather a periodic (e.g., quarterly) practice that is implemented within the organisation's trade compliance framework.

> ***The audit should not be a unique event, but rather a periodic practice that is implemented within the organisation's trade compliance framework.***

Although maintaining a strong internal control framework is the foundation of an export compliance programme, export compliance departments are often 'lean' – and corporate leadership may not recognise the true complexity of complying with the regulations. In addition to identifying risks, an audit programme can positively shine a light on these challenges by demonstrating what an organisation is doing well and where improvements can be made. An audit may even result in every export compliance professional's dream – getting the resources, staffing and technology tools needed to develop an exceptional export compliance programme.

For these reasons, as an organisation begins to plan the audit, it should consider how the findings will be used within the trade compliance framework and with respect to the business overall.

Planning the audit

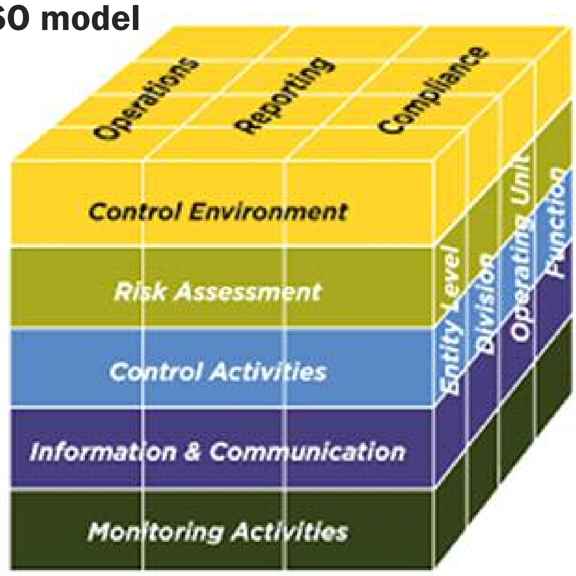
In planning the audit, the core team should define the objectives, outline the scope, identify the steps to be taken and reserve the required resources. The high-level scope and objectives should be established at the outset which will then later be refined upon completion of the risk assessment.

Complete a risk assessment

In approaching an audit, the organisation should conduct a risk assessment which identifies the highest areas of risk to the business.

Looking to the Committee of Sponsoring Organizations of the Treadway Commission ('COSO') – which defines itself as 'dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence' – risk assessments are one of the five components comprising an effective internal control system for any company. Other

The COSO model



components are (i) the control environment, (ii) control activities, (iii) information and communication, and (iv) monitoring activities. Please refer to the depiction of the COSO model (see illustration 'The COSO Model') , which has been adopted as the generally accepted framework for internal control and is widely recognised as the definitive standard against which organisations measure the effectiveness of their systems of internal control.[1]

Conducting an objective risk assessment is a valuable way to target areas for closer review as it will help focus time and resources on priority areas with the most risk. The risk assessment consists of developing a risk matrix that compares the likelihood of the event or activity against the possible impact. The likelihood criteria should consider factors such as volume/frequency of activity, existence of policies and processes, employee training in a given area, recent violations or voluntary disclosures, and newly implemented corrective actions. Assessing the potential impact requires a consideration of the possible results stemming from a compliance gap in the area. This can range from something relatively minor, such as a shipping delay, and can increase in severity to include fines and penalties levied on the organisation or complete denial of export privileges.

Specific topics included in the risk assessment will vary from one organisation to another, but some key areas for assessment that pertain to most exporting organisations include looking at jurisdiction classification determinations, technical data/ technology transfers, foreign-person employees, licences and authorisations, recordkeeping, restricted-party screening, international travel and visitor access. For those companies with items subject to the International Traffic in Arms Regulations ('ITAR'), other areas could include Part 130[2] reporting, Part 129[3] brokering and so forth. It is also helpful to review recent enforcement trends to identify topical areas of concern to the US government and to assess whether the organisation has any risks in those areas.

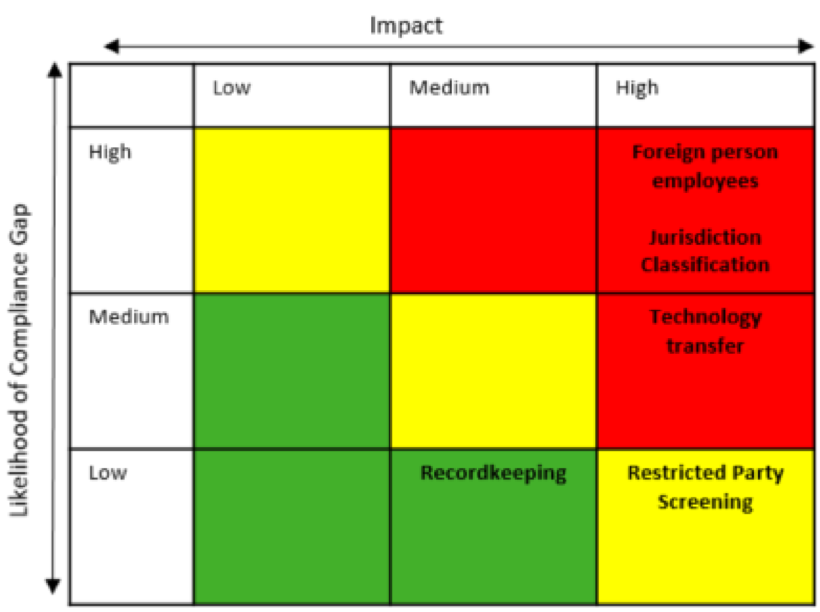
In the figure below, a fictional company has weighed possible compliance gaps for their organisation. In this example, the organisation does not have a robust jurisdiction-classification process or internal controls for foreign employees. Therefore, the likelihood of having a violation is high, as is the impact of a possible violation. In contrast, the organisation has a strong restricted-party screening process. As such, the likelihood of having a restricted-party screening violation is low, but the impact of a violation would be high.

The risk assessment can also be a valuable communication tool to gain management support for the time and resources that will need to be allocated for the audit. By clearly articulating the applicable risk(s) within the organisation, the trade compliance manager can bolster their case for conducting the review.

Refining the scope and objectives

Once a risk assessment has been conducted to identify the highest areas of risk throughout the organisation, the scope of the audit can be refined. Although this sounds like a simple step, it is important to agree upon the intent of the audit. This can range from conducting a high-level health check on a very narrowly focused matter,

Weighing up compliance gaps



 Audits

such as compliance with temporary hardware licences, or can entail a full-scale audit to validate compliance with all regulatory and organisational recordkeeping requirements. The audit management team also needs to determine if the review will be conducted company-wide or be focused on a specific division, location or product line. Conducting a risk assessment up front will help the team determine the appropriate audit scope to mitigate targeted risks and meet the overall objectives.

An additional aspect to consider is who will be conducting the review. There are certain areas where a self-assessment conducted by the local trade compliance group is appropriate. In other circumstances, it may be better for a corporate-level compliance group to be involved. There are also scenarios where engaging an external auditor may be the most objective way to identify compliance gaps, and in some cases involving US government penalties, the use of an external auditor is directed by the US government. Companies who have undergone consent agreements with the US Department of State Directorate of Defense Trade Controls often undergo multiple corporate-wide audits with some conducted by an external provider and other smaller reviews conducted internally.

External auditors are valuable in a number of ways. They can provide an objective perspective and provide insights into industry-leading practices. They can also provide additional resources for a larger-scale review, such as those required under consent agreements or government-directed audits. In the case where the headquarters or corporate office is reviewing business operations in multiple jurisdictions, it may be worthwhile to engage with a local auditor that understands the nuances of the local regulations and can speak the local language.

The purpose and scope of the review should be clearly communicated to the management of the organisation being reviewed to set expectations of what will be reviewed, including the resources and time commitments required. The scope, objectives and methodology of the review should be documented in an audit plan.

Conducting the review

Any review should include a combination of document review (policies, procedures and desktop instructions), employee interviews (including over-the-shoulder reviews), and transactional testing. Reviewing existing policies, procedures, and desktop instructions is needed to design the testing and develop interview questions. The review should confirm that the local guidance documents are aligned with both corporate policy and local regulatory requirements.

In multiple jurisdictions, it may be worthwhile to engage with a local auditor that understands the nuances of the local regulations and can speak the local language.

In conducting employee interviews, the auditor should gauge the employees' understanding of the existing policies and procedures and whether or not the day-to-day activity is being conducted accordingly. As technology becomes increasingly important in export compliance, another valuable exercise beyond soliciting verbal explanations is having the employee show the auditor how they use the automated tools to conduct transactions (e.g., walking the reviewer through their process in conducting a restricted-party screening).

Depending on the scope of the review, the auditor should endeavour to speak with a wide variety of employees, including those outside of trade compliance, such as shipping/ logistics, procurement, information technology ('IT'), security and/or engineering. For organisations that have network restrictions in place to limit access to export-controlled data, the auditor should do an over-the-shoulder review with IT under various profiles to understand how these network limitations are put in place.

For transactional testing, auditors should select a sampling of transactions to review that is representative of the organisation's trade profile. The sampling should include a broad range of criteria based on the volume and type of transactions involved.

For example, to conduct a review of hardware shipments, the auditor should select a mix of samples, including shipments authorised under varying government authorisations (or exceptions), and a diverse array of products, associated export classifications, export destinations, end-users, freight-forwarders and so forth. The testing should involve looking at the actual export declaration against the licence or authorisation, shipping paperwork and internal files/data to validate compliance with the regulations and relevant procedures.

Other types of testing involve reviewing licence reports, confirming restricted-party screening was conducted for all relevant transactions, testing the jurisdiction and classification determination, or reviewing visitor-access files and technology control plans. Another important area to review is training records and an assessment of whether the training was sufficient.

Reporting

As important as conducting the review itself is documenting the audit results. The level of documentation varies again based on the scope of the review and may be as simple as a few PowerPoint slides and as complex as a detailed report and testing logs.

It is important to refer back to the audit plan to verify that objectives have been met.

The report should include documentation of areas reviewed, deficiencies observed and recommend-ations for improvement.

After the audit

There are a number of different steps for the organisation to take after an audit. Typically, the audit will include a management response or development of a compliance-improvement plan. Before committing to corrective actions, the organisation may wish to conduct root-cause analysis to better understand the deficiencies and, as such, design better solutions. For errors identified in transactional testing, additional analysis should be done to assess whether the errors were clerical or systemic in nature.

Common examples of actions to be taken following a review include:

- Providing employees with additional training;
- Modifying or implementing new policies and procedures;
- Identifying and implementing new technology solutions; and
- Hiring additional team members or better distributing responsibilities throughout the organisation.

Links and notes

1 https://www.coso.org/Pages/aboutus.aspx.

2 https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework.

3 22 CFR Part 130.

4 22 CFR Part 129.

If the audit identifies a regulatory violation, the organisation also must determine if they want to submit a voluntary disclosure to the relevant government agency.

Corrective actions from the audit should be actionable and measurable. Follow-up is important to ensure that corrective actions are appropriately implemented. Audits may fail to achieve their purpose if corrective actions are not implemented or are only partially or incorrectly implemented.

Conclusion

In summary, a successful audit involves planning, performing, reporting and implementing improvements based on the results. Developing a risk assessment will help the audit team focus on key areas to review, and selecting the right team to perform the review at the right level will aid in gaining valuable insights about the overall health of the export compliance programme. Clearly, export compliance programmes should be dynamic, and on-going audits are a valuable tool to identify areas for improvement. Companies should keep in mind that an audit may result in additional training, modification of policies and procedures, identification of technology solutions, or providing justification for additional export compliance staff – all important aspects of the trade compliance life-cycle. Most notably, audits should be embraced as a tool to make improvements in an export compliance programme.

This article represents the views of the authors only and does not necessarily represent the views or professional advice of KPMG LLP.

Amie Ahanchian is a managing director, Brandon Barela is a manager and Sarah Blank is a senior associate in the Trade & Customs Services practice of KPMG LLP.

aahanchian@kpmg.com

bbarela@kpmg.com

sblank@kpmg.com

This article is reprinted from the March 2019 issue of *WorldECR*, the journal of export controls and sanctions.

For further information, visit **www.worldecr.com**