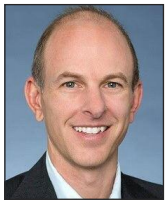
Utilising identity access management solutions to safeguard sensitive data




Export compliance professionals understand the importance of controlling physical access to certain areas and items. IAM solutions offer a way to manage variable access rights and control access to technology and data. Steven Brotherton and Amie Ahanchian describe the benefits of IAM for export compliance.

In today's business world, data can be both the driver of success and the cause of significant exposure for an organisation that experiences a data breach. In this article, the Global Export Controls and Sanctions Practice of KPMG LLP examines data access and protection by leveraging identity access management ('IAM') solutions and how those solutions can keep you ahead of the curve when it comes to data protection.

The IAM framework and maintaining effective control

As an export control officer, do you know where your company's data is stored? More importantly, are you familiar with how your data may be accessed? The world today provides instant access to infinite amounts of information, be it via a cloud-based service, or the phone you hold in your hand. Never has it been more important from a business perspective to control how your data is maintained, and furthermore accessed.

IAM solutions create a framework for data access by establishing roles and restrictions for various users based on their specific data needs. Specifically, IAM is based on various accounts and digital identities associated with those accounts to establish security parameters around your sensitive business data and controlled technology, ultimately allowing the right people to have the right access to the information required for their specific job function. Failure to create these parameters ultimately opens the door to a host of potentially irreparable damages, including not only loss of sensitive data information for criminal activities and insider threats, but export control violations as well.

It is likely that your company already employs some type of IAM component to restrict access to sensitive or proprietary data. For example, your payroll department has access to personnel records that an engineer would not need access to and, conversely, payroll would not need access to export-controlled technical data. Even further, an engineer working on one product may not need access to technical data on unrelated product lines, and IAM can be used to tailor an individual's access to only those areas of need. For the export control professional, taking a proactive approach to managing these access rights will assist in mitigation of inadvertent or deliberate attempts to view or obtain controlled data.

The need for IAM hits home when it comes to protecting controlled technology from unauthorised persons.

The intersection of IAM and export compliance

The need for IAM hits home when it comes to protecting controlled technology from unauthorised persons, including but not limited to certain employees, foreign and domestic visitors, and external business partners. The US government maintains stringent regulations that govern the export of controlled technical data or technology, namely the International Traffic in Arms Regulations ('ITAR') and the Export Administration Regulations ('EAR'), and non-compliance with these regulations can be damaging.

As a comparative example, imagine the distinct levels of physical access that employees working with defence articles in a facility governed by the

This article is reprinted from the July/August 2019 issue of WorldECR, the journal of export controls and sanctions.
www.worldecr.com

Typical data access levels for departmental functions

Publicly available	Proprietary	Regulatory Controlled	Classified
Publicly available information is generally accessed without limitation and available to all personnel across the entity	Proprietary information is generally limited to those that need access to support their job function, such as Human Resources	This level of data access should be restricted to export professionals responsible for compliance with various government regulations	The highest levels of data security are applied to employees that are cleared for access by the US government

ITAR may possess based on their role within the organisation, their job function, and their level of authorisation:

- Some professionals may only have access to the office space and conference rooms;
- Other employees, who work on the assembly line, may only require access to the manufacturing floor; and
- Select authorised personnel only may access the ITAR-restricted areas with controlled information.

At a facility, monitoring access to physical areas and products is fairly straightforward and achievable through the use of physical security protocols (e.g., locked doors, electronic access cards, cameras, signage), implemented ITAR procedures, and training.

Considering the fallout that would be caused by unauthorised exports or release of controlled data, it is of critical importance to design and maintain an IAM solution that implements user-verification gates at strategic checkpoints to establish proper role accounts, thereby protecting against any unauthorised releases. By first evaluating a user's credentials, the regulatory requirements and the company's business needs prior to provisioning any access, export compliance professionals can take their time to work with information technology ('IT') teams and set up the appropriate network profile. Once established, the company can have greater confidence that there are sufficient electronic controls in place to protect sensitive data from those that may not be authorised.

The graphic above provides an example of the level of access that a particular function may require.

Understanding sensitive and controlled data

The stakes for data loss increase when dealing with sensitive or controlled data, which is commonly understood as information that must be protected against unwarranted disclosure. Controlling access to sensitive data is necessary for a myriad of legal and ethical reasons, including control of proprietary and private data, and, in the US, for example, compliance with regulations such as the ITAR and EAR.

Technical data can have varying levels of control that will dictate specific limitations on who may have access to it as well as how it may be disseminated. Specifically, the release, or export of technical data or controlled technology may require a licence or other government authorisation depending on the end-user and ultimate end use or application of the data.

Technical data can have varying levels of control that will dictate specific limitations on who may have access to it as well as how it may be disseminated.

Exports of controlled technical data or technology can occur via many means, including email, oral communication or visual inspection and can occur both internationally, or within the United States. The latter, known as a 'deemed export', highlights the importance of knowing who you are dealing with when discussing or handling controlled data, because once the data has been released or discussed, the export has occurred.

All of this points to the importance of the export control professional maintaining an active presence in the ever-changing landscape of data protection. Given the regularity of technological advancement and the consistent updates to regulatory requirements, it is extremely important for the international trade practitioner to work in conjunction with IAM leadership to ensure the most current user rights are considered.

IAM solutions

Determining the level of IAM solutions that is right for your particular business structure is dependent upon a number of factors, including the type of data created or stored, your customer base, government control or classification level, and the requirements set forth by any governing agencies. Simple, process-based solutions exist that are tailorable to organisations of all sizes, and can support cross-functional implementation to allow multiple users from Human Resources, IT, Contracts, Security, etc. Access can be controlled by assigning user rights and entrusting administrative controls within a hierarchy of approvers.

When the make-up of a business requires more stringent protection, IAM solutions are predicated on utilising authoritative sources for users which enable the creation of the user and a process to define user's roles and privileges. In addition, management of the permissions and entitlements as the user moves within the organisation, and updating access rights as roles change, is more likely to be necessary when employing a large number of people and utilising a larger data-management network.

As organisations continue to develop their technologies, utilising multifaceted IAM solutions becomes critical. The use of IAM through biometric restrictions or dual-factor

Some examples of access restrictions

Principle of least privilege
Allow only view access, limiting the user only to view-data rights. Adding, updating, or amending data is not authorised.

Provisional access
User has access to certain operational systems like Windows, but not to development or testing platforms or mainframe systems.

Restricted access
Limiting users to specific roles that can access only certain parts of systems, databases, and information.

Multifactor authentication
Utilising a combination of something the user knows (like a password), something the user has (like a RSA token), and something the user is (like biometrics), to authenticate individuals and grant them access.

authentication is becoming more common as companies navigate the continually changing landscape of information control. Understanding the type of data you are trying to protect and the nuances of IAM will help you determine the best solutions for your company.

There are different ways to implement IAM policies to define and enforce role-based access control models, based on an organisation's specific needs (see above box, 'Some examples of access restrictions').

Whatever solution you deploy, keep in mind that without collaboration between the system administrators and export control practitioners, the solution may have gaps that give rise to potential violations and subject the company to increased risk and exposure or loss of data.

IAM key benefits

The values to be realised from a successful IAM system implementation are continually increasing. IAM solutions provide assurance that access controls are effectively implemented across your entity, and bring about a host of benefits including enhanced security features, threat-environment monitoring, and operational efficiency. Of paramount importance, maintaining an effective IAM system will allow your organisation to keep pace with ever-changing laws and regulations.

Implementing a well-defined process of identity lifecycle management and access provisioning to applications helps to act as a proactive measure and enables users to have necessary access based on the principles of least privilege, at the same time making the user efficient from the very get-go. It also empowers end-users by simplifying and automating application access requests and fulfilment processes.

A final benefit to IAM solution implementation is the ability to audit and monitor user access. Legal and regulatory requirements continue to stiffen, and periodic review for IAM internal processes and policies will drive a culture of compliance and assist with the identification of gaps in the system. Effective utilisation of data control and management systems allows for the tracking of all activity, including the source of access, user authentication, data removal, and approval activities.

Taking it one step further, companies may elect to link user-role accounts to physical security controls and/or meeting invites, providing greater assurance that users collaborating in certain buildings, floors, conference rooms, or even the attendees on a meeting invite, are authorised.

While this may seem like a tall order, chances are your company is already leveraging IAM solutions to some degree. With that in mind, export compliance professionals should reach out to IT professionals and explore ways to leverage the company's existing IAM framework to meet the company's export compliance needs.

Conclusion

The risks associated with the loss of sensitive information have become too great to ignore and the majority of companies have become resigned to the eventuality that a data breach is a matter of when, not if. Companies taking aggressive and proactive measures against this possibility, especially with respect to export controls, are subscribing to a smart tactic in mitigating unauthorised exposure to controlled data.

For the export control professional, it is not a matter of instituting a data protection solution from scratch, but enhancing existing systems and leveraging your international trade leadership to get the most out of your company's current IAM capabilities. Accordingly, IAM is a practical and accessible solution to ensure comprehensive controls are in place to protect against unapproved data access.

The authors would like to thank Jenna Glass, senior manager, and Ben Meyer, senior associate, for their contributions to this article.

Steven Brotherton is a principal and leader of the global export controls and sanctions service line and Amie Ahanchian is a managing director, global export controls and sanctions service line, in the Trade & Customs Services practice of KPMG LLP.

sbrotherton@kpmg.com
aahanchian@kpmg.com