How identity governance became a key compliance and risk control

Contents

Introduction

Organizations and individuals are increasingly using the new technologies of smart devices, cloud computing and social media to shop, to buy and deliver services and for other commercial purposes. In this always on interconnected world, Electronic Identities (IDs) provide the way for organizations to know their customers as well as to secure information systems and sensitive data. Identity Governance is the critical process that enables both of these objectives.

The distinction between governance and management is defined in COBIT 5.[1] Governance ensures that business needs for IT are clearly defined, agreed and satisfied in an appropriate way. Governance sets the priorities and the way in which decisions are made and it monitors performance and compliance against the agreed objectives. Governance is distinct from management in that management plans, builds, runs and monitors activities in alignment with the direction set by governance to achieve the objectives.

Based upon this definition, identity governance sets the business objectives for the control of access to IT systems and data. It forms the foundation upon which the processes and technologies for the management of identities and access to IT systems are chosen, built, and operated. It provides the justification for the way in which access to the IT systems is controlled and the actions to be taken if these controls are breached.

One of the major objectives of Identity Governance is to mitigate risks. These risks include the theft of information, fraud through the improper manipulation of systems and data, as well as the subversion of IT systems. Examples include financial fraud, theft of intellectual property, and the unauthorized release of information that is sensitive or confidential. The large number of recent high profile incidents demonstrate the need to address these issues—in all industries and sectors. The leakage of privacy-related customer data and industrial espionage is a problem across the board.

Governance challenges

The always on interconnected world, provides a growing opportunity to those organizations that are able to exploit these evolving technologies. The number of connected individuals and devices has grown exponentially and exploiting the data from these is an important factor to successfully identifying and connecting with customers, partners and suppliers. This data can come directly from the devices themselves as well as from a variety of sources such as social media. Behind these data lie the individuals, and being able to recognize these individuals is a major challenge. Simply knowing just the demographics of who is watching a TV show can allow a TV channel to sell targeted advertising. The connections between an individual's email, Facebook and twitter handle allow an e-commerce seller to recognize positive or negative feedback from a customer that just bought something. It enables the seller to take action immediately to rectify a problem before it goes viral. It also allows the seller to better target future marketing.

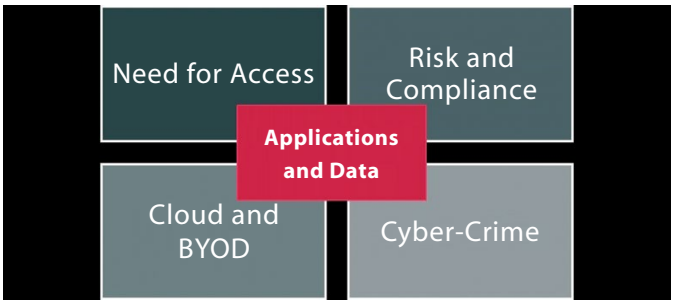

Figure 1. Challenges

Within the organization and between organizations, individuals require access to the systems and data that they need to perform their jobs. As businesses outsource services and work directly with partners and suppliers, they are faced with the additional problem of needing to give access to individuals outside of the organizational boundary. Wherever the individual is located and whatever organization they are part of, their access needs to be managed and controlled to lower the risk of fraud and ensure compliance. Governing the way this access is assigned, managed and monitored is essential pre-requisite for the security of business.

Organizations need to comply with an ever increasing range of laws and regulations. Although many of these do not directly involve IT systems, these systems are frequently involved because they hold regulated and controlled data. To prove compliance requires an audit to confirm that the access to this data is properly managed. In the absence of good identity governance these audits can be time consuming, expensive and painful.

The audits take time because:

- They involve examining all of the access rights and activities on all of the in scope systems.
- They are expensive because of the work needed to transform the technical data extracted from the systems into a form that can be understood by the auditors.
- They are painful because the audit process involves many business roles beyond IT Risk and Compliance; for example business managers may need to confirm the access rights of their subordinates.

These audit and compliance challenges are increasing because of the way in which access has expanded outside of the organization and because of the many different ways in which systems and data are now accessed.

This extension of access beyond the organizational boundaries has made it necessary to trust the identity and access management processes and technologies used by third parties. It is no longer sufficient for the organization to control its own processes and technologies, it must be able to verify that those used by its partners and suppliers are adequate. This means that identity governance needs to include the assurance of the processes and technologies used by the third parties.

The use of mobile phones, tablets and other devices by employees, associates and partners to access organizational systems and data has created a new set of risks. The security of these devices is usually outside the control of the organization and the user is often unaware of the technical risks associated with downloaded apps and the use of public Wi-Fi networks. The devices are frequently lost and stolen together with any downloaded data. Data is also being transferred to these devices and between organizations using public cloud services. This is often done in order to enable the employees to "get the job done" in spite of organizational access controls.

Cyber-crime is becoming an increasing challenge with the frequency and sophistication of cyber-attacks growing. Even worse data breaches are often detected by outsiders before the organization affected detects that they have been attacked. These cyber-attacks on organizations now routinely involve multiple stages designed to overcome the strength of modern organizational network defenses. Since it is becoming almost impossible for illegitimate traffic to penetrate an organization's technical network defenses, attacks now target the theft of legitimate credentials or dupe an individual into carrying malicious software into the organization through social engineering. As a consequence of this cyber-defense must now assume that the organizational network has been breached. Cyber-intelligence needs to monitor the apparently legitimate behavior of individuals to and correlate this with other factors to detect abnormal patterns of usage. Identity governance provides data which can help with this.

The evolution of identity technologies has made it difficult for lines of business to understand what the IT departments are doing to control access. The scale of the number of IDs for each employee is already daunting; many commonly have more

than five sets of credentials and sometimes more than twenty sets. Complexity is further increased through the need for outsiders, such as partners and suppliers, to have access to internal systems as well as the needs for insiders to have access to systems for externally provided services like travel. Identity governance is needed to help to manage this area of complexity.

IT security and compliance groups within an organization often find it a challenge to understand the real underlying business needs for security and compliance so that they can design the appropriate technical controls. Furthermore governance of this area has often been added as an afterthought rather than as an essential foundation for security and compliance. Governance is vital to ensure that the technologies and the processes are related to the business needs and that everything is prioritized and dealt with on the basis of these needs.

Every access permission or entitlement represents a potential risk through misuse, malice, or mistake. Organizations face the challenge of relating these risks to business objectives and of managing them in an environment where there are increasing numbers of individuals with access rights and the ways in which access can be made is also expanding. In the past many organizations have invested in identity management projects that have helped IT operations, however these have not yielded tangible benefits for the business. Identity and access governance can help to manage these access related risks in a way that leverages the existing investments.

Value from Identity Governance

Good identity governance adds business value and reduces costs in a number of different ways. It focusses effort on business objectives; it improves understanding and helps to facilitate communication between the different parts of an organization. It saves costs through ensuring that solutions meet business needs and through streamlining and automating processes.

It reduces risk through better controls and monitoring to avoid theft, fraud and misuse of information. It helps to protect the organization against cyber-crime through a better understanding of legitimate activities. It provides a practical and effective approach to compliance. It improves risk management by providing a way measure how the implementation of policies and controls improves risk over time.

Identity governance facilitates communication between the organization's board of directors, lines of business, IT security and IT service providers. The organizational board sets the overall priorities for governance and compliance and these, in turn, set the primary objectives for the control of access. The line of business managers set the objectives for specific systems and understand the sensitivity and value of the data these systems contain. Thus they have a key input into the requirements to control access to that data. Neither of the previous objectives are technical, nor are the people setting them technicians. These objectives need to be translated into a technical specification and implementation by IT services and IT security staff. Identity governance ensures that the technical architecture and components can be related back to the business requirement and so their need and priority can be understood by all the stakeholders.

Identity governance ensures that the processes and technologies to manage identity and access are focused and built based on real business need. This helps to accelerate the delivery of IT systems and to reduce their cost. By focusing on the real business needs rather than the latest technology it ensures that the IT systems are scoped correctly, built using appropriate technology and implement the appropriate controls; and as a consequence helps to avoid function creep in identity projects.

One of the consequential benefits of better communication and understanding is that it allows the business to take on higher value activities with confidence even though there may also

be a higher risk. Examples include the use of emerging IT technologies like cloud services as well as new business approaches involving third parties. Without this joint understanding it is easy for the IT security group to take an overly cautious approach that either deters business from taking action or causes the business to bypass the IT organization altogether and deal direct with a third party.

The processes involved in managing security compliance are complex and time consuming. These processes involve many different parts of an organization well beyond the IT group. Good governance together with the use of the right tools to automate and simplify these process can save time and effort as well as improving the compliance posture.

The leakage of sensitive information can be very expensive both financially and in terms of loss of reputation. The cost of the loss of IPR can be measured in tens of millions of dollars[2] and compliance penalties can be equally severe. Good identity governance can reduce these risks it two ways: firstly it can reduce the probability of the loss occurring through closer control over the allocation of access rights; secondly it can improve the likelihood of early detection through monitoring of user activity to spot abnormal patterns of behavior.

Improved Teamwork

On the face of it, it may seem that providing individuals with the access to the systems that they need to do their work is a simple task. This is not a one-time task but a lifecycle and there are many complexities involved in achieving and maintaining this goal. One important factor is teamwork; there are usually many different people across the organization that are responsible for aspects of the process. Identity governance helps to enable all these people to work together in a coordinated manner. Because the complexities of the IT technologies and systems involved, identity governance tools are essential to make this teamwork possible and avoid the "pain chain" illustrated below:

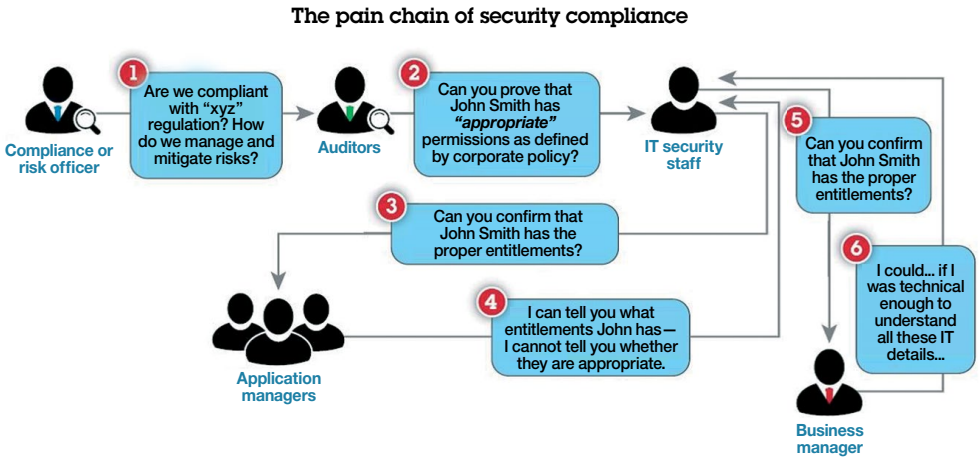

Figure 2. Compliance Pain Chain

The following list of typical stakeholders found in an organization together with their responsibilities provides an illustration of the complexities involved showing the need for help to support team working:

- The owners of data and applications services are responsible for classifying the sensitivity of data including any legal or regulatory requirements around this data. This is a key input into assessing risk and setting access controls.
- The line of business managers are responsible for defining the access that individuals within their organization should have to applications and data. They are also responsible for periodically confirming that the actual access rights possessed by individuals are correct as part of compliance processes.
- The HR department, in conjunction with line management, is responsible for performing background checks on new employees, initiating the on-boarding processes that give the access to IT systems, initiating processes to change access rights when employees change job functions, and for initiating the off-boarding processes that remove access rights for employees leaving the organization.
- IT management is responsible for ensuring the identity and access infrastructure is installed, configured and functioning correctly. It is specifically responsible for managing the access to the privileged accounts needed to manage the IT infrastructure, databases and applications. IT management may also be responsible for running the Help Desk which can accept requests for changes to access rights and to perform account and password reset.
- IT Security is responsible for ensuring that the IT infrastructure, applications and data are secure. These processes involve configuring the systems to remove vulnerabilities, detecting anomalous activities and responding to incidents.
- The legal department is responsible for setting up legal agreements, e.g., identity federation with partner and supplier organizations as required by corporate management or line of business owners. The IT department is responsible for the infrastructure required for this. Lines of business owners are also responsible for the control of access to systems by external users like customers and partners.
- Internal and external auditors are responsible for ensuring that the controls on access to organizational systems and data are appropriate to the risks and are compliant with the laws and regulations that apply. These responsibilities now extend beyond the organization's internal processes to assuring the controls of partners and suppliers with access to the organization's systems.

Better Processes

To achieve the business objectives, the stakeholders illustrated above need to work together on a number of processes. The complexity of these processes means that tools are required to ensure that they are carried out correctly, efficiently and in a timely manner. These processes encompass a wide range of activities and the tools to support these activities must be integrated to obtain the benefits. Identity governance tools provide the core around which the multiple identity and access management processes must be integrated to achieve the business objectives.

Without identity governance the cost of these processes will be unnecessarily high and their efficiency will be too low. For example a large financial services organization found that using the right tools reduced the time take to perform regular access rights reviews from months to days.

The following list illustrates some of the processes that are involved:

- Provisioning of identities and access rights: when individuals join and organization they need access to the IT systems and applications before they can perform their jobs. Good identity governance ensures that these entitlements are provided appropriately, securely and without delay.
- Verification of IDs – to avoid misuse of systems and leakage of data it is important to ensure that every ID can be related to a person or system with a current genuine need for access. When an ID for a person is created there must be a way to check that the person actually exists and that they are entitled to this ID. When a person leaves or changes their job the IDs that are no longer required should be disabled or removed. IDs without an associated person are often called "orphan accounts" and these represent a risk; tools should be used to discover these and trigger remedial action.
- Roles and Entitlements – for people to do their job or perform their business role they need to have appropriate access to the systems, applications and data that are required. Achieving and maintaining this simple objective can be very complex. Firstly a person may have primary and secondary roles – that is to say that they may do more than one job on certain occasions. For example one person may act as a deputy for another person when the latter is absent. Secondly the way in which business entitlements are defined to an IT system is often complex leading to the inter-relationships between business functions and technical access rights being difficult to understand and tools are needed to help.
- Separation of duties (SoD) – this is a well understood business concept that is intended to reduce fraud. For example if a person who is responsible for placing orders for goods is also able to authorize payment for those goods there is a risk that they could fraudulently order and pay for something that is not delivered. A further example is where the separation of duties depends upon the circumstances; for example a manager may be permitted to authorize the expenses of a subordinate but not where the subordinate has bought something for the manager. This adds another layer of complexity onto the assignment of entitlements to individuals. Once again tools are needed to help to ensure that the entitlements of individuals match the organization's policies for separation of duties.
- Certification: regulations often require that the rights of individuals to access data and systems should be periodically reviewed and recertified as being appropriate. This process can be time consuming and difficult for the managers involved unless appropriate tools are provided. These tools should make it easy for the non-technical managers to understand the match between the business need and the technical details.

Cost Effective Compliance

In the past, some organizations attempted to build their identity governance on a theoretical basis of who should have access to what. This approach was not successful because it did not take account of the practical realities and complexities of how organizations actually operate. For example a manufacturer of luxury goods failed a compliance audit because of excessive access

rights; each user had on average 800,000 individual access entitlements. When an automated analysis of the entitlements actually used was performed, it was found that the number of entitlements needed could be reduced by a factor of twenty.

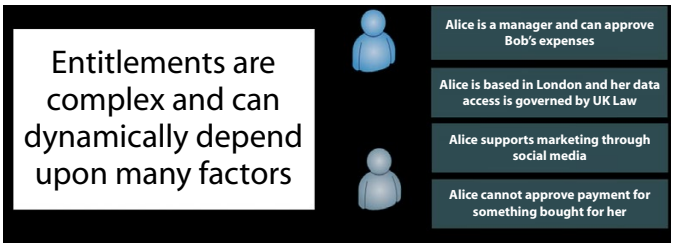

Figure 3. Complexity of Entitlements

Auditing access rights and controlling separation of duties can be very difficult without the correct identity governance tools. These complexities can arise because an individual performs more than one role. Each role may require access to several systems with each involving large numbers of entitlements. The different roles, or simply the vast number of entitlements, may lead to SoD conflicts which may be almost impossible to spot without tools to help. This challenge can be even more complex because of the dynamic nature of the conflicts, some of which may only occur under certain circumstances; this is illustrated in the diagram above. A practical approach that can improve compliance, and reduce audit costs is to start by understanding the way in which entitlements are actually being used and to build upon this.

The existing IT systems and applications in most organizations are already operating with some form of access controls. These controls may or may not be meeting the business objectives for security and compliance but they do allow the organization to function. Creating a new theoretical set of access control rules usually leads to unexpected problems with the existing business processes. To avoid this problem and to gain insight into what is really happening within the business it is important that identity governance uses tools that allow the status-quo to be analyzed before making changes.

These tools can help to analyze the access rights that individuals have in several ways. The existing access rights and entitlements are analyzed with respect to the official job functions of the individuals possessing the rights. In this way the actual rights assigned for particular business roles are compared with the theoretical rights based on business analysis which helps to avoid interrupting the business by mistakenly removing essential entitlements. It helps by providing a better understanding of how the business is really operating. It also facilitates the identification of "outliers", that is to say individuals with anomalous access rights; these may stem from a previous role or even help to prevent attempted fraud.

This approach can lead to a better compliance posture by starting with an audit of how the business is actually using entitlements to operate. This audit enables the business to identify and correct real risks without the need for complete re-engineering of entitlements. The result is a leaner operation and less likelihood of a failed external audit.

Improved Security Intelligence

The essential characteristic of Security Intelligence is that cyber-attacks are detected before damage is done or data is stolen. The traditional approach which has focused on network activity has not been successful in this activity because cyber-criminals have found ways to mimic apparently legitimate user activities. To counter this emerging threat the security operations center must take into account user activity and pro-actively seek out these threats amongst the vast amount of legitimate activities.

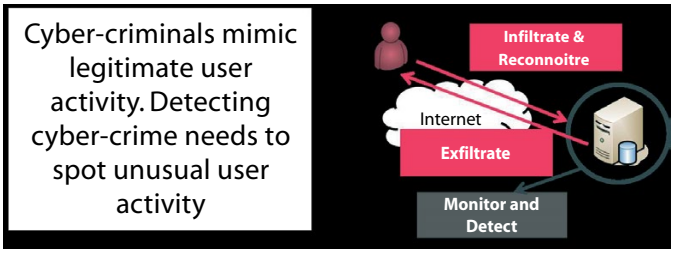

Figure 4. Cyber Crime

Identity governance provides an important foundation for security intelligence. Cyber-criminals now exploit human and technical weaknesses to infiltrate organizational networks and to use apparently legitimate protocols and access rights to access and exfiltrate data. In order to detect this apparently legitimate activity, you need a detailed understanding of individuals' access rights and normal patterns of access to be combined with the traditional network activity monitoring data. To achieve this requires data monitoring and analysis tools with immense scalability, because of the volumes of data involved, together with detailed up to date knowledge of the tools and techniques used by the cyber-criminals.

Improved Risk Management

Every access right is a potential risk and the greater the number of users, the larger the number of access rights, the higher the access risk. The objective of risk management is to reduce the business impact of a risk or the probability that it will occur. Both of these dimensions are very difficult to define and measure, in addition many technical controls are hard to relate to business objectives. In practice, access risk can be considered to be a combination of factors that can be used as key performance indicators associated with business groups, processes and applications to visualize how business risk changes over time in response to the implementation of policies and controls.

Figure 5. Manage Risk against business objectives

Identity governance provides intelligence and compliance controls that previous Identity Management technology could not address. Identity governance incorporates measurable access risk controls that can help to set policies and to better drive activities such as access review, privilege management and the management of separation of duties. Performance as measured against these controls can also be more readily related to the underlying business objectives. Identity and access governance technology achieves this by leveraging the existing Identity Management environment, complementing and extending the work that the organization has already undertaken in this area.

IBM Identity Governance and Intelligence

IBM Identity Governance and Intelligence is a core component of the IBM Identity and Access Management software portfolio. It is designed to help organizations effectively manage identities and application access by bridging the gaps across compliance, business and IT infrastructure operations.

The IBM Security threat-aware identity and access management portfolio helps to protect identity as a new perimeter with controls to manage and report on user entitlements and access activities. It provides user metrics and audit reports that can be used to can deal more quickly and efficiently with the complexities of compliance and inappropriate user access.

IBM Identity Governance and Intelligence can help organizations mitigate access risks and SoD violations with business-driven identity governance and end-to-end user lifecycle management. It provides an integrated, streamlined approach for managing user roles, access policies and risk, ensuring that appropriate levels of access are applied and enforced across enterprise and cloud applications. The solution automates the administration of user access privileges across an organization's resources, throughout the entire identity management lifecycle—from initial on-boarding to final de-provisioning. By delivering improved visibility into how access is being utilized, it helps to answer critical compliance questions such as "Who has access to what resources and when?" and "How did users get access to resources and why?"

IBM Identity Governance and Intelligence products enable managers to govern and manage users' roles and privileges across the extended enterprise, including cloud environments. These threat-aware solutions help organizations avoid separation of duties violations, support business policies and eliminate inappropriate user access. By controlling and auditing user activity and strengthening access controls, organizations can improve governance, prevent insider threats and identity fraud and achieve regulatory compliance.

Summary

Identity governance is essential for organizations to ensure the security of their IT systems and data as well as compliance with laws and regulations. Identity governance enables organizations manage IT related business risk and enable business compliance in consistent, efficient and effective manner. It adds value, reduces costs and improves security in the following ways:

- It ensures that the appropriate access rights are provided in a timely manner to the individuals that need them.
- It ensures that the individuals have their access rights assigned in a way that minimizes opportunities for misuse and fraud.
- It helps to avoid data leakage by ensuring that data and applications can only be accessed by authorized individuals.
- It enables cost effective compliance with laws and regulations by ensuring that the access rights of individuals meet the requirements for compliance.
- It ensures that individuals are accountable for their use of IT systems and data.
- It provides the transparency over access rights and activities that are needed to ensure compliance with laws and regulations.
- It improves that management of access related risks.

For more information

To learn more about IBM Security solutions for identity and access management, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
May 2016

Please Recycle

[1] http://www.isaca.org/cobit/pages/default.aspx

[2] http://www.mynewsdesk.com/uk/news/mi5-gchq-william-hague-speak-up-in-espionage-the-1st-in-the-cyber-series-broadcast-by-bbc-radio-4-62969

WGW03119-USEN-01