RSA

WHITE PAPER

Beyond the Checkbox

A sustainable approach to access certification

Review Risks

Every organization has employees who need access to its critical information resources, and many also have contractors, partners, vendors and customers who need a variety of types and levels of access. Each point of access is a source of potential business and compliance risk.

The process by which access roles and entitlements are authorized, reviewed, certified or recertified is critical to an organization's ability to meet compliance standards and to protect itself against access-related risks. These are continuing challenges that require a sustainable process. But establishing a genuinely sustainable access certification process has proven difficult for many large organizations.

While it is relatively easy to provision new users with initial access to applications and other information resources, it is not so easy to ensure over time that their access entitlements are changed appropriately as their duties, employment status or contractor status change.

Today's provisioning systems are able to handle onboarding and offboarding efficiently, but they are typically not designed to ensure that each user has just the right level of access at any given time (what is needed to do his or her job—no more, no less) or to ensure that each user's access conforms to all applicable compliance requirements and internal policies, even as the user's functional responsibilities and relationships within the organization change.

Many organizations are still trying to manage access certification with resource-intensive or homegrown spreadsheet-based solutions that are error-prone and time-consuming to develop and maintain. With such systems in place, IT managers are hard-pressed to keep up with who has access to what. Business managers find themselves asked to certify user access rights without a clear understanding of current entitlements. Furthermore, the information provided to business managers to use in certification provides no context for determining whether user entitlements are appropriate for their business roles. And internal audit and compliance teams struggle to make sure that a complex web of regulatory requirements and company policies is adhered to in a consistent fashion.

The result is often an unnecessarily high cost of compliance and an increased risk of compliance violations, security breaches and operational errors that can have serious consequences for an organization.

Any system capable of managing the risks associated with information access must be not only accurate, but also simple and manageable enough to make compliance sustainable. Fortunately, technology is available that makes it possible to achieve a successful, sustainable process by:

1. Establishing full visibility of user entitlements and roles
2. Automating authorization and access certification
3. Providing a business-centric view of entitlements in relationship to roles
4. Maintaining a system of record for evidence of compliance
5. Automating change management and entitlement remediation

The benefits of such a process include:

- Cost avoidance through access risk management
- Cost reduction from process automation
- Accountability for governing access being driven into the organization

The problem with entitlements

Here's a scenario that occurs every day—in one form or another—throughout the business world:

> XYZ Financial Services, a major brokerage company, creates a new wealth management division. XYZ staffs the new division by hiring 100 new employees and transferring 100 current employees from the brokerage operation. Each of the newly hired wealth management employees gets access to a set of applications associated with his or her job title, as well as certain levels of functionality within XYZ's new investment management system. The employees coming from the brokerage side of the business are issued the same entitlements, but their access to the brokerage-side functionality remains active even though it is no longer needed.
>
> This now represents not only a separation-of-duties compliance violation under the Gramm-Leach-Bliley Act (GLBA), but also a potential security problem as well. In the months that follow, one of the transferred employees uses his brokerage-side access entitlements to discover a pending acquisition and then executes stock trades on behalf of a client to take advantage of the information. When the insider trading is discovered, the employee and XYZ Financial Services become targets of a criminal investigation and the firm is embroiled in a public relations nightmare.

This type of problem isn't unique to financial services firms, or even to the private sector. In every large organization, employees come and go, get transferred and are reassigned. Turnover among contractors, vendors, business partners and customers is continual, and each of these changes poses a risk to the organization when the person involved has or needs access to enterprise information resources.

This risk was exacerbated beginning in 2020 by pandemic-related remote work, furloughs and other changes, and it continues now as more employees and others continue to work from home or other locations beyond the traditionally secured network perimeter.

Although many organizations can manage onboarding new users and offboarding users at the termination of their relationship with the organization, many fail to properly manage the changes that are required or appropriate when a user's responsibilities or other status variables change. In the example above, the central issue was dealing with access change management. Onboarding new employees and granting new entitlements to the reassigned employees was not the problem; it was the failure to remove the access entitlements no longer needed by the employees.

It is also worth noting that the company in the example above not only committed a compliance violation, but also incurred business risks when an employee took advantage of the failure of the organization's access certification process. In the long run, the cost of the latter in terms of financial liabilities and damage to the organization's reputation could far exceed any regulatory penalties.

Making sure that all users have only the minimum access rights required to perform a specific function, and that no user has access entitlements that are unnecessary, in violation of regulatory requirements or company policies, or otherwise inappropriate, requires a continuous process in which every entitlement is properly authorized, certified and regularly recertified. Compliance is not a one-time event, and neither is access authorization and certification.

Regulatory compliance: an obvious challenge

Publicly held companies in the United States are subject to many types of regulations including Sarbanes-Oxley, GLBA, the Health Insurance Portability and Accountability Act (HIPAA), the US Patriot Act, and California SB 1386 and its equivalent state disclosure laws.

Industry-specific regulations apply in financial services (Basel II Accord), healthcare, energy (NERC, FERC) and many other sectors. Companies that conduct business internationally have additional regulations to consider. Canada (PIPEDA), the European Union (GDPR) and a host of Asian and Latin American nations have their own privacy regulations, for example, and Japan has its equivalent to Sarbanes-Oxley (J-SOX).

Regulatory bodies are well aware of the frequency with which large organizations still fail to maintain the necessary access control procedures, which is why access control is so often a focal point of their audits.

In highly regulated industries, organizations operate under intense compliance scrutiny with exposure to serious consequences in the event of a security breach. Even in so-called "non-regulated" industries, regulatory requirements are considerable, and senior executives may be subject to stiff fines and even imprisonment for compliance failure with Sarbanes-Oxley.

Complying with this regulatory mosaic is a challenge, but there is no alternative.

Compliance is not the whole story

Fines and other penalties for compliance failure are not the entire sum of an organization's risk exposure when access controls are inadequate. The costs of a security breach can dwarf any regulatory sanctions. The immediate financial impact of fraud or an act of vandalism, ransom, terrorist tactics or other malicious activity can be enormous, and the damage to an organization's public image can be crippling. Even in a secure and compliant environment, it is still possible to issue inappropriate access entitlements that can lead to mistakes, resulting in data loss or service interruptions.

That is why achieving regulatory compliance is no guarantee of the best possible risk management. An organization's access control system can be in full compliance with all applicable regulations and still be vulnerable to serious, unacceptable security risks that could have been mitigated or eliminated with the proper security controls.

In addition to viewing access control as a defensive tool, many organizations have discovered that an effective system can also overcome certain types of operating inefficiencies, thereby creating a business advantage. For example, a good control system can enable an enterprise to extend access to employees or contractors in remote locations in a way that leads to more efficient business transactions without incurring additional security or compliance risks. It may also accelerate the process of developing new applications or lead to improvements in customer service, so access governance must not become a roadblock to success.

Creating a sustainable access certification process

Creating an access control process in which access entitlements are properly authorized, reviewed, certified or recertified is now an achievable goal. A sustainable process—one that takes hold, works and is maintained—requires the capabilities reviewed below.

Establishing full visibility of user entitlements and roles

Getting a handle on access certification begins with gaining the ability to see what user entitlements currently exist throughout the enterprise. This was once virtually impossible in large organizations, where the number of applications and users can run into the tens of thousands, and the number of individual user entitlements into the billions—and changing constantly. It is also not unusual to find business managers within large organizations relying on inconsistently maintained spreadsheets and other ad hoc, often inaccurate systems for reviewing the access entitlements for which they are responsible.

Fortunately, technology is available that can provide a "snapshot" of all user entitlements throughout a large organization at any point in time by collecting access-related data from all repositories or applications, aggregating it and then normalizing it into reports that IT personnel, business managers and auditors can easily digest.

Automating authorization and access certification

Having made this information available to the business managers in an easily understood format, it is then necessary to provide a simple, automated way for those managers to certify (or decertify) existing roles and their corresponding entitlements or to authorize new ones. It is critical to make this process quick and easy to ensure the line of business (LOB) managers' cooperation. Automating the process will also help to ensure accuracy.

Each manager or application owner may be using a different system for keeping track of who has access to what, so the possibilities of inaccuracies and oversights that lead to security vulnerabilities are nearly endless. There are compliance issues as well. When business managers have to rely on spreadsheets or other manual systems for keeping track of the access certifications for which they are responsible, it can be difficult to maintain an auditable record of who certified what entitlements and authorized what changes. In addition, auditors look at the underlying processes that support access certification and recertification and not just at the reports that are generated. A process that is inconsistent from one manager to the next or that lacks an audit trail could be flagged as a compliance violation.

A faulty access certification process can also lead to problems even when security and compliance have been ensured. An unintentional error made by an employee who has been issued an inappropriate entitlement can have serious—even catastrophic— consequences. For example, a software developer who has been given access to the organization's IT production system due to a managerial oversight could introduce faulty code into an application server and cause it to crash. If the application is mission-critical, the risks introduced to the organization can have a material impact on business performance.

Automated data collection, aggregation and normalization eliminate these problems and open the door to considerable reduction in compliance certification overhead as well.

Providing a business-centric view of user entitlements and roles

To properly certify an access entitlement, a business manager must be able to understand what the entitlement is, whether it is appropriate for a user's role in the organization, and who has it or will have it as a result of the certification. In addition, the manager must know or otherwise be guided by the relevant regulatory requirements and internal policies that need to be enforced to ensure good access governance.

User entitlement data is typically recorded in cryptic security syntax that is meaningless to non-technical managers. When the information isn't expressed in business terms and cannot be easily interpreted, managers can't tell who has access to what, and many of them resort to rubber-stamping access certification and recertification reports. Solutions are available that can provide business-centric descriptions of entitlements to ensure that managers understand exactly what they are certifying. In addition, mapping roles as a set of entitlements that relate to a particular business process provides the context to better understand whether access is appropriate and necessary to perform a person's function.

When a business manager authorizes an entitlement—before the access is granted— the entitlement should be matched against all available regulations and internal organizational policies to ensure that there are no violations or conflicts. This process can also be automated, to ensure accuracy and to prevent this task from becoming burdensome to business managers, IT staff, or any audit or compliance personnel.

Maintaining a system of record for evidence of compliance

Many homegrown access request systems are efficient for creating access but aren't designed with governance or compliance in mind. They may make the request process more efficient by automating the workflow for granting access, but they do not address the issue of providing evidence of compliance.

As a result, access entitlements may be created without the appropriate audit trails, and it may be difficult, if not impossible, to answer questions about who approved an entitlement, whether appropriate reviews have been conducted and by whom, and whether exceptions have been resolved. In addition, many provisioning systems are not designed for the fine-grained entitlement administration that is required for access certification. For example, an ERP or CRM system creates a user account, but can't create roles for related fine-grained entitlements, which are especially important for applications that are in scope for separation-of-duties requirements.

An automated access governance system is a central repository for all access-related information that concerns IT policies and compliance requirements including:

- Who has access to what?
- Who certified a role and each user entitlement?
- Records of regular reviews of access rights for appropriateness
- Records of exceptions raised, with audit trails showing how these issues were resolved

Such a system can then provide actual evidence of compliance.

It is essential to maintain collaboration with internal audit and compliance teams to make sure that all existing access entitlements and all new access requests are filtered through the proper context of regulations and policies. A properly automated system can make it relatively easy for auditing and compliance personnel to input current regulatory requirements and internal policies, and to ensure that violations are prevented. In effect, this gets the regulations and policies out of the three-ring binder and into the daily operating practice of the organization.

Additionally, this gives external auditors a centralized system of record to review that houses all the information necessary to attest to the effectiveness of controls governing access. This will in turn further reduce the cost of compliance.

Automating change management and entitlement remediation

Access certification in any large organization is in constant flux and never stable. New hires, transfers, promotions, reassignments, terminations, mergers, acquisitions and new regulations are just some of the changes that require continual attention. Remediation is the process by which changes to user access privileges resulting from access certification reviews are passed via a workflow to the target application or application owner.

In an automated access governance system, change requests can be tracked to completion as a work order. For example, Manager A rejects an entitlement for Employee B because Employee B's job role and responsibilities have changed. The rejection is logged and tracked within the access governance system and then passed directly into the work queue of the person or system responsible for provisioning that application. The administrator or provisioning system receives this work request and makes the change. The access governance system confirms completion of the change, providing an auditable end-to-end view of the entire transaction.

In addition to establishing policies and procedures to ensure that each of these kinds of events triggers appropriate action within the access certification system (for example, requiring that employees who leave the company have all their access entitlements removed immediately), it is necessary to create a process for conducting regular, periodic recertifications. When this process is automated, it can be both accurate and relatively easy for all involved. Efforts can also be focused on the riskiest categories of entitlement, since Sarbanes-Oxley guidance has shifted from strict mandates to allowing organizations to use risk-based controls.

Benefits

The benefits of a sustainable access certification process fall into three categories:

Cost avoidance

As mentioned earlier, the potential cost of regulatory sanctions is substantial, but the potential cost of dealing with a security breach, lost data or access-related service interruptions is astronomical. Remember, even an unintentional error made by an employee who has been issued an inappropriate entitlement can have serious, even catastrophic, consequences. Properly managing the business risks associated with user access is critical to ensure that unforeseen costs, fines and penalties are avoided.

Cost reduction

An automated system for access governance can greatly reduce the employee time and other overhead associated with managing access certification. A manual approach is labor-intensive in terms of the IT security team. Managing the certification process with business units and applications is also labor-intensive when manual tools (such as spreadsheets) or homegrown systems are used. Automation streamlines the process and will reduce the efforts required for certifying access compliance from a staffing level perspective.

Accountability

A clear definition of who is responsible for what and an auditable trail of who has approved what create a degree of accountability that serves as the glue that holds the entire access certification process together. Accountability for governing access is not the sole responsibility of the IT security team. But business unit managers are not experts in regulatory compliance or legal issues, which is the domain and responsibility of the compliance and audit team. It is essential that a collaborative approach is used for access governance, where all key stakeholders (IT security, business managers, and the audit and compliance team) participate, and accountability is fully understood.

RSA: Access certification philosophy

RSA believes information security teams need to collaborate with business units and with compliance and audit teams to achieve good security governance across the organization and manage the risk of inappropriate access to information resources. We have focused on the automation of the many critical, often still manual, tasks associated with access governance, risk and compliance management across the enterprise. To respond rapidly to security and regulatory demands, organizations need enterprise access governance. Our governance and lifecycle solution meets this need by providing robust, auditable business processes that enable policy-based automation and deliver visibility into who has access to what; how they got that access; whether they should have access; and whether security and compliance objectives are being met.

SecurID Governance & Lifecycle:

- Makes LOB managers key participants in access governance
- Supports all entitlements and roles and enables roles-based governance
- Provides reports, certifications and analytics that are easily understood by business users
- Enables and tracks entitlement changes
- Facilitates fast deployment and massive scale
- Reduces risk due to unauthorized access and compliance violations
- Integrates with identity management and change management systems

SecurID Governance & Lifecycle supports automated remediation and auditing of user access privileges across the organization through native integration with an organization's existing identity management and IT change management infrastructure.

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.