GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Identity and Access Management

The Institute of Internal Auditors

What is GTAG?

Prepared by The Institute of Internal Auditors (The IIA), each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology (IT) management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

Guide 1: *Information Technology Controls*

Guide 2: *Change and Patch Management Controls: Critical for Organizational Success*

Guide 3: *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*

Guide 4: *Management of IT Auditing*

Guide 5: *Managing and Auditing Privacy Risks*

Guide 6: *Managing and Auditing IT Vulnerabilities*

Guide 7: *Information Technology Outsourcing*

Guide 8: *Auditing Application Controls*

Visit The IIA's Web site at www.theiia.org/technology to download the entire series.

Identity and Access Management

Project Leader

Sajay Rai, Ernst & Young LLP

Authors

Frank Bresz, Ernst & Young LLP

Tim Renshaw, Ernst & Young LLP

Jeffrey Rozek, Ernst & Young LLP

Torpey White, Goldenberg Rosenthal LLP

November 2007

Copyright © 2007 by The Institute of Internal Auditors, 247 Maitland Ave., Altamonte Springs, FL 32701-4201. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission from the publisher.

The IIA publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

Table of Contents

1. EXECUTIVE SUMMARY 1

2. INTRODUCTION 2
   2.1 Business Drivers 2
   2.2 Identity and Access Management Concepts 3
   2.3 Adoption Risks 4

3. DEFINITION OF KEY CONCEPTS 5
   3.1 Identity Management vs. Entitlement Management 6
   3.2 Identity and Access Management Components 6
   3.3 Access Rights and Entitlements 6
   3.4 Provisioning Process 7
   3.5 Administration of Identities and Access Rights Process 9
   3.6 Enforcement Process 10
   3.7 Use of Technology in IAM 10

4. THE ROLE OF INTERNAL AUDITORS 12
   4.1 Current IAM Processes 12
   4.2 Auditing IAM 14

APPENDIX A: IAM REVIEW CHECKLIST 17

APPENDIX B: ADDITIONAL INFORMATION 22

GLOSSARY 23

ABOUT THE AUTHORS 24

1. Executive Summary

Identity and access management (IAM) is the process of managing who has access to what information over time. This cross-functional activity involves the creation of distinct identities for individuals and systems, as well as the association of system and application-level accounts to these identities.

IAM processes are used to initiate, capture, record, and manage the user identities and related access permissions to the organization's proprietary information. These users may extend beyond corporate employees. For instance, users could include vendors, customers, floor machines, generic administrator accounts, and electronic physical access badges. The means used by the organization to facilitate the administration of user accounts and to implement proper controls around data security form the foundation of IAM.

Although many executives view IAM as an information technology (IT) function, this process affects every business unit throughout the organization. For instance, executives need to feel comfortable that a process exists for managing access to company resources and that the risks inherent in the process have been addressed. Business units need to know what IAM is and how to manage it effectively. IT departments need to understand how IAM can support business processes and then provide sound solutions that meet corporate objectives without exposing the company to undue risks. Addressing all of these needs requires a solid understanding of fundamental IAM concepts.

In addition, information must be obtained from business and IT management to understand the current state of companywide IAM processes. A strategy, then, can be developed that is based on how closely existing processes align with the organization's business objectives, risk appetite, and needs.

Matters to be considered when developing an IAM strategy include:

- The risks associated with IAM and how they are addressed.
- The needs of the organization.
- How to start looking at IAM within the organization and what an effective IAM process looks like.
- The process for identifying users and the number of users present within the organization.
- The process for authenticating users.
- The access permissions that are granted to users.
- Whether users are inappropriately accessing IT resources.
- The process for tracking and recording user activity.

As an organization changes, so too should its use of IAM processes. Therefore, as changes take place, management should be cautious that the IAM process does not become too unwieldy and unmanageable or expose the organization to undue risk due to the improper use of IT assets.

The Role of Internal Auditors

Because IAM touches every part of the organization — from accessing a facility's front door to retrieving corporate banking and financial information — chief audit executives (CAEs) may wonder how organizations can control access more effectively to gain a better understanding of the magnitude of IAM. For instance, to effectively control access, managers must first know the physical and logical entry points through which access can be obtained. Poor or loosely controlled IAM processes may lead to organizational regulatory noncompliance and an inability to determine whether company data is being misused.

As a result, the CAE should be involved in development of the organization's IAM strategy. The CAE brings a unique perspective on how IAM processes can increase the effectiveness of access controls, while also providing greater visibility for auditors into the operation of these controls.

The purpose of this GTAG is to provide insight into what IAM means to an organization and to suggest internal audit areas for investigation. In addition to involvement in strategy development, the CAE has a responsibility to ask business and IT management what IAM processes are currently in place and how they are being administered. While this document is not to be used as the definitive resource for IAM, it can assist CAEs and other internal auditors in understanding, analyzing, and monitoring their organization's IAM processes.

2. Introduction

For years, organizations have faced the complex problem of managing identities and credentials for their technology resources. What used to be a simple issue that was confined within the walls of the data center has become a growing and exponentially complex problem facing organizations of all sizes.

For instance, many large organizations are unable to effectively manage the identities and access permissions granted to users, especially in distributed IT environments. Over the last several years, IT departments have built system administration (SA) groups to manage the multitude of servers, databases, and desktops the organization uses. However, even with the creation of SA groups, managing access to the organization's resources remains a challenge.

Even with this expansion, human resources and manual processes are sometimes unable to handle the complex tasks and excessive administrative overhead needed to manage user identities within the organization. What's more, in recent years regulatory requirements have added complexity and increased external scrutiny of access management processes. These regulatory requirements and prudent business practices have led organizations to grant individuals access at the most granular feasible level, forcing managers to determine what specific rights are needed, rather than granting users access to resources they do not actually need to do their jobs.

Although what is commonly referred to as IAM has become an industry-accepted term, there are many definitions in use, depending on the industry, product vendor, or professional consultant. However, the core premise remains the same. This publication does not claim to have the correct authoritative definition. Rather, it blends many of the definitions that have been presented in the IT industry.

2.1 Business Drivers

According to a recent International Data Group (IDG) Forecast Report[1], spending on IAM and related systems is expected to grow rapidly. Within the United States, this increase is being driven primarily by the U.S. Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach-Bliley Act (GLBA) of 1999, the Basel II Accord, and other industry-specific regulations. For instance, the financial services industry is subject to guidance specifying the use of multiple sets of credentials (i.e., multifactor authentication). This forecast report predicts that the IAM global marketplace will increase by at least 10 percent per year to US $5 billion by 2010. Thus, many organizations will make IAM a primary IT project in the future.

With this surge, it is important to examine the many reasons why organizations embark on IAM projects. These include:

- Improved regulatory compliance.
- Reduced information security risk.
- Reduced IT operating and development costs.
- Improved operating efficiencies and transparency.
- Improved user satisfaction.
- Increased effectiveness of key business initiatives.

2.1.1 Improved Regulatory Compliance

Without overstating the effects of the regulations mentioned in the previous paragraph, it is important to note that Sarbanes-Oxley, HIPAA, GLBA, Basel II, and other regulations have significantly impacted organizations worldwide. However, while IAM initiatives have helped fill the gaps related to system access controls, they may not have gone far enough. Many companywide IAM initiatives are merely stopgaps to regulatory compliance. Although this approach to dealing with IAM may pass an audit, it may hinder the organization in the future as the IAM program becomes overly complex, inoperable, and costly. Organizations also must be aware that IAM programs frequently collect personal information about system users. Therefore, these programs need to be aligned carefully with privacy and data protection laws, such as the European Union's Directive on Data Protection of 1995.

2.1.2 Reduced Information Security Risk

A key driver to successful IAM implementation is the improved risk posture that comes from the implementation of better identity and access controls. By knowing who has access to what, and how access is directly relevant to a particular job or function, IAM improves the strength of the organization's overall control environment.

In many organizations, the removal of user access rights or access rights for a digital identity can take up to three to four months. This may present an unacceptable risk to the organization, especially if an individual is able to continue accessing company systems and resources during the access removal period. For example, anecdotal evidence indicates that some users, such as contractors, continue to have access rights for years, which results in the continued unauthorized access to systems and exposure of the organization's infrastructure to avoidable hacking attempts.

2.1.3 Reduced IT Operating and Development Costs

Ironically, the proliferation of automated systems can negatively impact worker efficiency due to the different sign-on mechanisms used. As a result, workers must remember or carry a variety of credentials that change frequently. For example, a typical employee may have a username and password for their desktop, a different username and password to gain access to other systems, several more usernames and passwords for different desktop and browser applications, and

[1] IDG Report #204639: *Worldwide Identity and Access Management 2006-2010 Forecast Update With Submarket Segments*, December 2006.

a personal identification number (i.e., PIN) with a one-time use password for remote access.

Considering the sheer number of these credentials, multiplied by their frequently expiring passwords, credential maintenance can become overly complex and unreasonably challenging for users. This often results in users' dissatisfaction with the process and forgotten passwords. This scenario degrades employee efficiency and significantly impacts support functions such as the help desk, which administer these credentials and handle forgotten password calls.

The proliferation of automated systems can also add significant operating costs by reproducing user identity directories and databases, thus resulting in poor performance and increased costs, most of which are hidden. For example, many organizations are faced with the following circumstances:

- A lack of defined and automated approval workflows, resulting in a best guess by an administrative assistant when initiating the provisioning process and handling access requests.
- An increased number of help desk calls, many of which are related to identity and access support, such as password-reset requests.
- Having new employees wait a week or longer to obtain baseline access to IT systems, such as e-mail and network resources.
- Not documenting access requirements by role, so users have to make several follow-up calls to get the access they need.

2.1.4 Improved Operating Efficiencies and Transparency

Having a well-defined process for managing access to information can greatly enhance a company's operating efficiency. Many times, organizations struggle with getting users the access they require to perform their job functions. For instance, requests are forwarded to various members of the IT or administration team who may not know what access or information a user is requesting or has a business need to obtain. Additionally, without a defined process, requests may go unfulfilled or be performed incorrectly, resulting in additional work on the part of the IT or administration team.

Therefore, implementing a defined IAM process can greatly enhance the process' efficiency. In large organizations, the appropriate use of enabling IAM technologies can ensure a request is routed to the correct person for approval or to the appropriate system configuration or automated provisioning system. In addition, access requests that take weeks to be completed can be reduced to days, while compliance reporting for these approvals is enhanced through the use of defined approval workflows within the established IAM process.

2.1.5 Improved User Satisfaction

Besides the operating efficiencies mentioned earlier, implementing an effective IAM process can enable users to identify the access they need, submit the request to the appropriate approver, and quickly gain access to work information. This, in turn, helps to reduce user frustration, which is particularly important as new employees are hired (e.g., when new team members are provided timely access to perform their job functions, they are productive sooner).

2.1.6 Increased Effectiveness of Key Business Initiatives

Often, certain business initiatives require access rights to be changed. These typically include joint ventures, outsourcing partnerships, divestitures, mergers, and acquisitions. For companies that are involved in these activities, the ability to quickly provide access to the appropriate levels of information can enhance the activity's success significantly. Conversely, without a well-defined process it may be difficult to determine whether the correct level of access was granted or removed. For example, during a joint venture or merger, timely access to appropriate information and timely termination of access to certain company resources are critical.

2.2 Identity and Access Management Concepts

IAM is a complex process consisting of various policies, procedures, activities, and technologies that require the coordination of many companywide groups such as human resources and IT. This guide will help CAEs understand the different components of IAM, enabling the subject to be more easily understood. For a more thorough definition of these components, please refer to the glossary at the end of this guide.

Fundamentally, IAM attempts to address three important questions:

1. **Who has access to what information?** A robust identity and access management system will help a company not only to manage digital identities, but to manage the access to resources, applications, and information these identities require as well.
2. **Is the access appropriate for the job being performed?** This element takes on two facets. First, is this access correct and defined appropriately to support a specific job function? Second, does access to a particular resource conflict with other access rights, thus posing a potential segregation of duties problem?
3. **Is the access and activity monitored, logged, and reported appropriately?** In addition to benefiting the user through efficiency gains, IAM processes should be designed in a manner that supports regulatory compliance. One of the larger regulatory realities under Sarbanes-Oxley and other regulations is that access rights must be defined, documented, monitored, logged, and reported appropriately.

2.3 Adoption Risks

The creation of an IAM process poses the potential for changes in personnel and current business activities and the need for capital investment. Introduction of IAM processes into an organization can expose it to new risks while mitigating existing ones. These risks need to be examined and understood by the organization as it implements new or modified IAM processes. Specifically, the following should be considered:

- **Organization complacency.** Many organizations are happy to continue performing certain processes the same way they always have, even if the status quo is inefficient or inadequate from a control perspective.
- **Participation.** Any major project requires additional time and the commitment of various resources to ensure the project's success. If the organization does not dedicate sufficient time, project activities are at risk of inadequate completion.
- **Planning.** Successful projects require well laid-out plans, milestones for delivery, and processes for scoping change management to set expectations regarding resource commitments and timelines.
- **Communication.** IAM project objectives, planned activities, and resource requirements must be expressed to the appropriate stakeholders. Without this communication, the individuals who need to be involved in the project will not be able to provide the appropriate input.
- **Incorporation of all systems into the process.** IAM projects are complex and tend to take a substantial amount of time to complete. Trying to bring many computer systems into the IAM framework at once can be overbearing and unsuccessful. Prioritizing key business risk areas and the system resources affected by the process are good targets for initial scope.
- **Process complexity.** In line with the complacency risk, making a revised process too complex will affect its success. For instance, users may try to circumvent the process or create their own.
- **Making the process too weak.** If the IAM process is weakly defined, nebulous, or open to user interpretation, it will encourage others to create sub-variant practices that do not effectively use the IAM process.
- **Lack of enforcement.** As part of the IAM process' implementation, governance, and use, proper enforcement activities enable it to operate as designed. If users are allowed to employ varied processes or circumvent established ones, the project's overall success can be jeopardized.

While some of these risks can be mitigated or eliminated, they must be identified, understood, and prioritized before, during, and after the IAM process is defined.

3. Definition of Key Concepts

The concepts below will be addressed in the following sections:

- **Identity** — the element or combination of elements used to uniquely describe a person or machine. It can be what you know, such as a password or a personal identification (ID) number; what you have, such as an ID card, security token, or software token; who you are, such as a fingerprint or retinal pattern; or any combination of these elements.
- **Access** — the information representing the rights that the identity was granted. These information access rights can be granted to allow users to perform transactional functions at various levels. Some examples of transactional functions are copy, transfer, add, change, delete, review, approve, read-only, and cancel.
- **Entitlements** — the collection of access rights to perform transactional functions. Note: The term entitlements is used occasionally and synonymously with access rights.

When the concept of identities is discussed, many executives typically think of human users. However, it is important to remember that there are also service accounts, machine identities, and other non-human identities that must be managed. Failure to control any of these identities and the access they have can be detrimental to an organization's overall control framework.

For identities to become part of an organization's DNA and access management system, they need to pass through several stages. These stages are:

- **Provisioning.** Provisioning refers to an identity's creation, change, termination, validation, approval, propagation, and communication. This process varies in breadth and length of time to complete based on the specific needs of the organization. In addition, this process should be governed by a company-specific and universally applied policy statement that is written and maintained by the IT department with input from other business units.
- **Identity management.** Identity management should be a part of ongoing companywide activities. It includes the establishment of an IAM strategy; administration of IAM policy statement changes; establishment of identity and password parameters; management of manual or automated IAM systems and processes; and periodic monitoring, auditing, reconciliation, and reporting of IAM systems.
- **Enforcement.** Enforcement includes the authentication, authorization, and logging of identities as they are used within the organization's IT systems. The enforcement of access rights primarily occurs through automated processes or mechanisms.

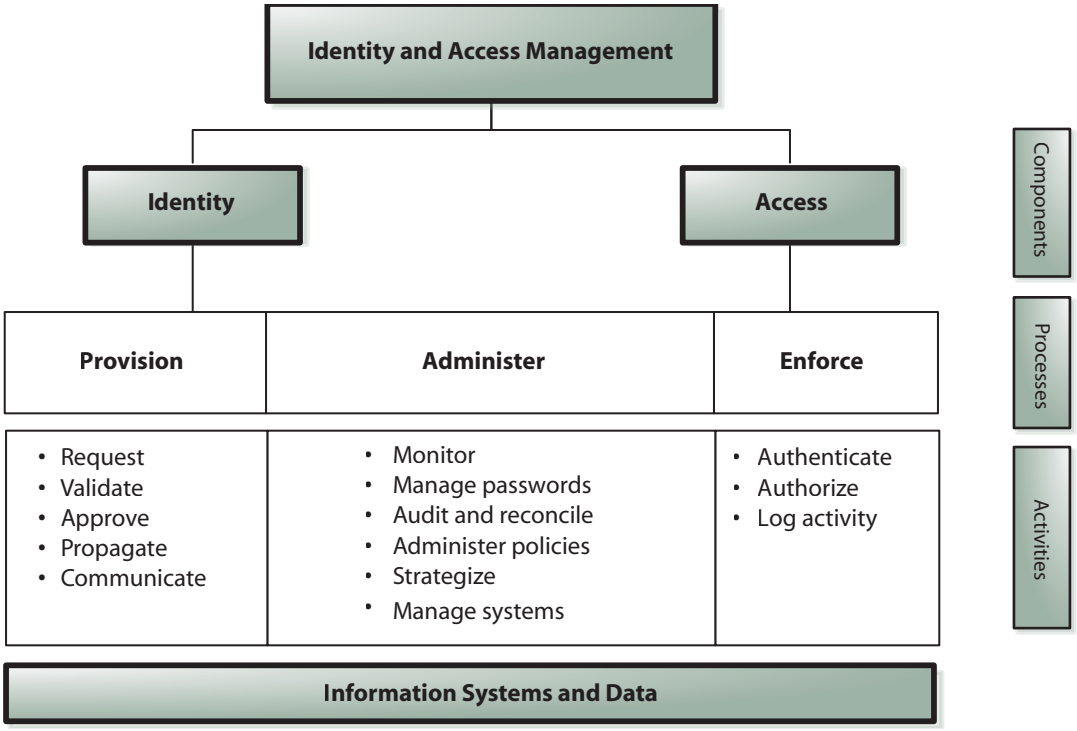

Figure 1. Relationships between IAM components and key concepts

3.1 Identity Management vs. Entitlement Management

3.1.1 Identity and Access Management Process

An IAM process should be designed to initiate, modify, track, record, and terminate the specific identifiers associated with each account, whether human or nonhuman, by making use of the organization's IT resources. The organization, then, should use its IAM process to manage these identifiers and their respective association with user accounts. As a result, the IAM process should be designed to incorporate the applications a user account needs to access and how identifiers — if different between applications — are associated with the user. Figure 1 demonstrates how identity and access management components relate to one another.

3.1.2 Entitlement Management

As part of the IAM process, entitlement management should be designed to initiate, modify, track, record, and terminate the entitlements or access permissions assigned to user accounts. Regardless of the methodology the organization employs to group user accounts into similar functions (e.g., work groups, roles, or profiles), entitlements for each user need to be managed properly. Therefore, the organization should conduct periodic reviews of access rights to detect situations where users accumulate entitlements as they move within the organization or where users are assigned improper entitlements. To accomplish reviews of access rights, business units need to request reports of access rights and communicate needed changes through the proper IAM mechanisms to the IT department.

One component of a properly designed entitlement management process is a segregation of duties analysis. This can prevent assignment of entitlement combinations that provide an individual with inappropriate access across a business process or detect conflicts that currently exist.

3.2 Identity and Access Management Components

3.2.1 Identity Types

Identities take many forms within an organization, and all types of identities should be considered in an identity management process.

Identity types include, but are not limited to, any or all of the following:

- Employees who use IT resources.
- Vendors (e.g., subcontractors).
- IT devices (e.g., hardware devices that perform functions similar to a user, such as fixed and mobile applications).
- Application service accounts (e.g., pre-defined accounts provided by the software vendor).
- Machine accounts (e.g., IT hardware devices that perform functions within and across IT environments or applications, such as a floor machine).
- Functional or batch accounts (e.g., those used to execute batch processes, such as overnight report generating batches).

When auditing the identities present in the organization, auditors should determine whether specific and universally applied identifiers are associated with each identity type. This allows different rules to apply to the management and review procedures associated with different types of accounts. For instance, a batch account may be subject to different policies and may require a different type of review than a user account.

3.2.2 Onboarding

Once the need for an identity has been determined, the identity has to be created in the IT environment. The manual or automated process used to create this identity is called onboarding, which involves the creation of an identity's profile and the necessary information required to describe the identity.

3.2.3 Offboarding

Offboarding is the opposite of onboarding. During this process, identities that no longer require access rights to the IT environment are identified, disabled or deactivated, reviewed to ensure they are inactive, and deleted from the IT environment after a predetermined period of time.

3.3 Access Rights and Entitlements

3.3.1 Identity Access or Entitlement Changes

Provisioning and Access Right Changes

When a user is granted an identity through the provisioning process, an evaluation of the access rights being granted or changed should be part of the business owner's approval and the IT department's review of the access request. While the IT department should not be held responsible for the approval of user identities, they should be involved in the process because they have a better understanding of how the access rights granted on various IT systems interact with one another.

Non-person Account Access Rights

Many applications, databases, and tools require the use of functional accounts. These accounts are not generally used for authentication by a specific user but rather for communication between two different system components. For instance, most database management systems (DBMSs) require the systems on which they are hosted to have specific

accounts created and active for the DBMS to operate. Therefore, the organization needs to have a proper way to request the generation of these accounts, limit their access to appropriate entitlements only, monitor who has access to account authentication credentials, and revoke the accounts when they are no longer needed.

3.3.2 Granting Access Rights to Privileged Accounts

Granting Privileged Account Access to an Identity

Privileged accounts are normally assigned to the person within the IT department responsible for administering IT systems, including network devices and applications, and the overall IT infrastructure. Typically, these users are entrusted by the organization with a level of access that permits them to make high-level and sometimes undocumented changes to the IT environment. To prevent unnecessary or inappropriate access to these accounts, the organization should include a section in its IAM policy statement that addresses their proper provisioning, administration, and enforcement.

Monitoring Privileged Accounts

Privileged accounts exist in every organization. In many companies, these accounts are placed in the hands of trusted individuals due to the risk they represent. Despite the level of trust placed in these individuals, appropriate IT management should periodically perform some of the following steps:

- Review the list of users with privileged access.
- Review, whenever possible, the activities of privileged accounts.
- Review online activity of these privileged accounts for inappropriate transmission of outbound sensitive data and for inappropriate introduction of unapproved applications.

3.3.3 Segregation of duties

Conflicts

During the provisioning process, the approvers of access requests should evaluate whether the request will cause a segregation of duty conflict. Additionally, when establishing or changing a user's identity, the IT department may note a potential segregation of duty conflict. In this case, the IT department should notify the business owner or approver of the problem. Performing a segregation of duty analysis before granting additional access to an account can be automated and used as a preventive control.

Periodic Monitoring of Access Rights

As part of its IAM monitoring process, the organization should establish a methodology to periodically review the access rights granted to all identities residing in its IT environment. This review, while facilitated by the IT department, should be conducted primarily by the organization with approvals received from each responsible business owner. In addition, privileged and IT account identities should be reviewed by an appropriate manager or system owner.

3.4 Provisioning Process

A logical workflow progression that addresses the provisioning process is presented in Figure 2.

3.4.1 Access Request

The process for requesting the creation, deletion, or changes to an identity should be defined in a procedure that details:

- How requests are to be made for the different types of identities (e.g., manual, electronic, or calls to the help desk).
- Where the requests need to be routed.
- Specific timeframes for making requests.
- Fulfillment expectations.

3.4.2 Approval

An identity request should be subject to a multistep approval process. The initial request approval should be granted by the authorized individual directly responsible for supervising the requestor's activities. Also, the approval should occur prior to when the request is submitted to the IT department. Once the first level of approval is granted, a second level of approval may be necessary and should be granted from the application owner. After the appropriate approvals have been secured, the request should be routed to the IT department or appropriate system for fulfillment.

3.4.3 Propagation and Identity Creation

Once creation of the identity is approved in a manner that is in compliance with the organization's policies, the identity will be created by an individual in the IT department or by an automated application controlled within the IT department. The following items should be taken into consideration when creating the identity:

- The requestor's function within the organization.
- How the identity will be used.
- Whether access granted to the identity owner will be based on roles, rules, or user-specific needs.
- Whether the identity can be replicated from an existing role or a new role will need to be created to meet the user's needs.

The creation of the identity requires an understanding of how it will be used, the software applications it will use, and any schedule restrictions the identity may be subject to or need relief from. The identity also should be created with a corresponding password containing restrictions that are specific to the application and in compliance with the organization's policy statement.

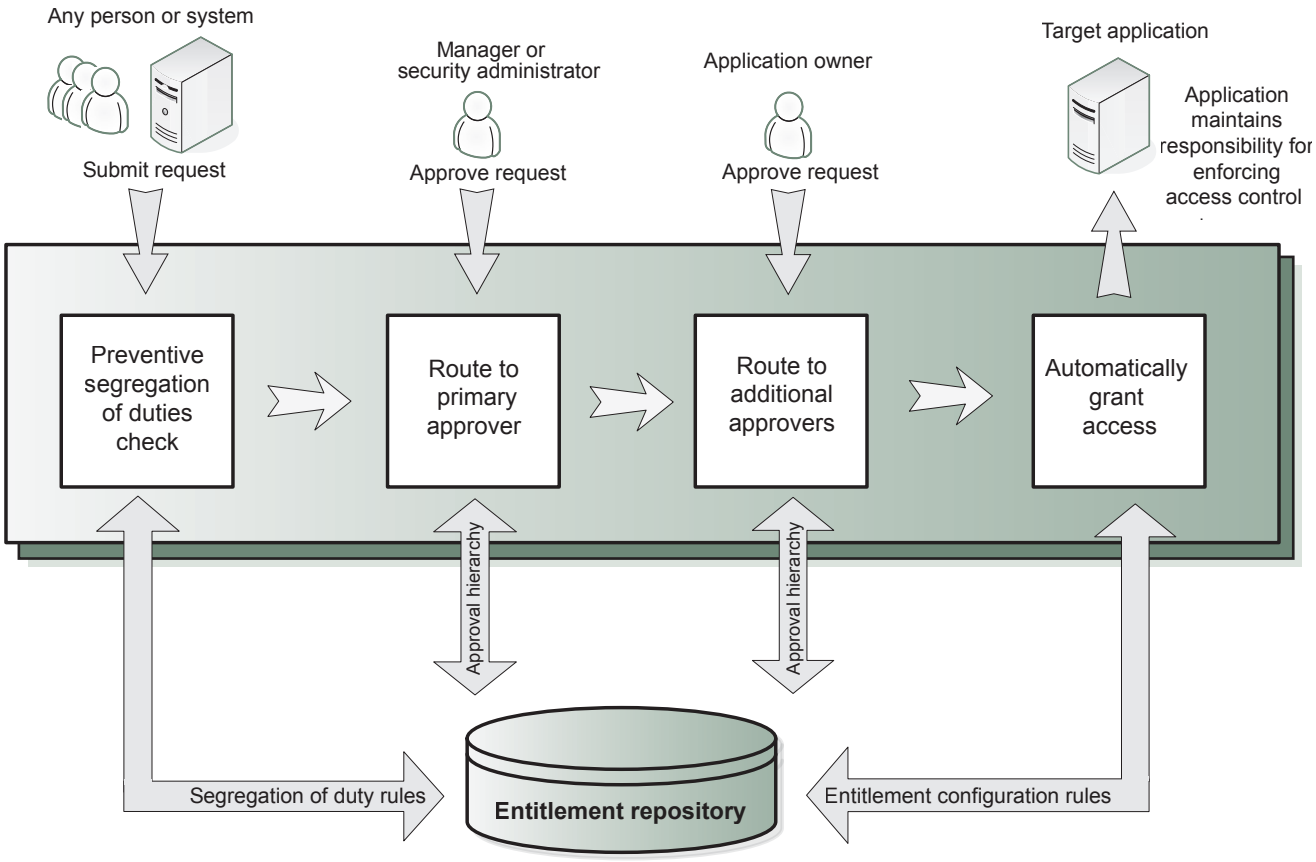

Figure 2. Diagram of an automated provisioning process logical flow

When granting an identity to a person, many IT departments assign a temporary password that the user must change during the initial login attempt.

During this part of the IAM process, the entitlements or access rights assigned to the identity should be evaluated in conjunction with the identity's functional role in the organization to determine whether conflict of interest issues regarding segregation of duties arise.

3.4.4 Communication

As part of its policy statement, the organization should define how to communicate the creation, deletion, and change of user identities. The organization also should establish a centralized location or department, separate from IT, to initiate identity communications to IT.

In addition, the IT department should use a mechanism to receive and send communications related to the creation and deletion of, or changes to, an identity. The means of communication can take the form of an automated message, verbal message, or paper documentation.

Any communication regarding the identity should conform to the organization's data classification policy. When communicating about an identity's creation or changes through electronic or paper means, staff must be cognizant of any data classification restrictions and requirements for identity configuration information. Communications that contain a password, for instance, may need to be sent in sealed envelopes, encrypted e-mail messages, or other secure methods. The organization should also require users to change the password after its first use to prevent misuse of the identity and to mitigate risks associated with its interception by an unauthorized party.

3.4.5 Logging

An entitlement repository is a system that tracks the privileges granted to users over time and records access requests, approvals, start and end dates, and the details related to the specific access being granted. This data can be used when auditing access, performing user entitlement reviews, and determining whether access activities were approved.

The logging-generated data should be maintained for a defined period and then destroyed. The retention period should be based on the nature of the access being logged, any regulatory and audit requirements, corporate policies, and data storage constraints.

3.5 Administration of Identities and Access Rights Process

3.5.1 Periodic Audit and Reconciliation of Identities and Entitlements

Periodic Audits

To evaluate the design and effectiveness of an organization's IAM system, periodic auditing of the process is necessary. Audit frequency should be determined as part of the annual audit planning process, which stems from internal audit's annual risk assessment. The audits themselves should consist of:

- An identification of highest to lowest risk identity concentration.
- A re-examination of the IAM process design.
- An examination of the IAM process operating effectiveness.
- A review of the provisioning process, which encompasses the evaluation of a sample of identities representing a cross-section of those that were active for any portion of the audit period.
- An examination of IAM enforcement activity effectiveness.
- An examination of IAM administrative activity effectiveness.

Segregation of Duties

IAM processes and methodologies should not be the only controls used to prevent user identities from having inappropriate access. Consequently, the organization should incorporate some method for verifying or reconciling user identities and their corresponding access rights with the actual access rights for which these identities were originally approved. This reconciliation process may reveal some of the following:

- User identities possess access rights that match the rights they were approved to have.
- User identities did not have their access rights reviewed and approved as frequently as expected.
- User identities possess access rights that do not match the rights they were approved to have.
- User identities associated with terminated or deactivated users still reside in the IT environment.
- Users who need to be issued identities and granted access rights did not have access requested or approved.

If the verification and reconciliation process reveals identities and access rights that are misaligned, the organization should have a way to report these problems, determine any corrective actions, and acquire necessary approvals to correct these deficiencies.

Entitlement Reviews

Mature IAM processes can facilitate the access review activities of managers and application owners. Managers can review the access granted to their direct reports, while application owners can review the access granted to all individuals who use the application to identify and revoke potentially inappropriate access. This review process should be performed at least annually or more frequently for critical applications or high-risk individuals.

3.5.2 Policy Statement Administration

The organization should have a means to periodically review and revise the IAM policy statement to ensure it reflects relevant current processes and activities.

3.5.3 IAM Strategy

Either the IT department or a strategy group within the organization should establish a comprehensive plan for initiating, changing, and sustaining IAM policies, components, processes, and activities. The plan should address how the organization will proceed with the IAM process, as well as present and future IAM risks; whether IAM processes and related activities will consist of manual or electronic solutions; and whether all areas of the organization will be incorporated in the IAM process.

3.5.4 IAM System Administration

Once IAM processes have been established within the organization, they need to be maintained through some means — manually, electronically, or a combination of both. The maintenance of the IAM process primarily involves infrastructure-related administration. This encompasses items such as determining:

- Where IAM processes are centralized.
- Whether technology will be used to administer IAM processes and, if so, where this technology will be housed.
- Who will be the IT and line of business owners of IAM.
- How changes will be documented and logged.

3.5.5 End-user Password Administration

After an identity is created, an initial password is usually assigned. This initial password may be generated manually or electronically and is communicated to the user by the IT department. Therefore, although IAM refers to the identities and access rights of users, issuing and maintaining user passwords must be considered as well. Password parameters, structures, and proper use should be detailed in the organization's security policy.

Maintaining user passwords is a vital component of an effective IAM process. Password maintenance includes conducting the following tasks:

- Issuing initial passwords.

- Communicating passwords to users.
- Resetting passwords for locked-out users.
- Reviewing password activities that comply with the organization's policy guidelines.
- Reviewing for easy-to-guess passwords, which can lead to potential misuse of the organization's IT assets.

3.5.6 Storage and Handling Considerations

The IAM process also needs to address how the organization will store, report, protect, and manage identities and access rights. When storing identities and access rights, the organization needs to be cognizant of where they will reside; how they will be viewed and reported (e.g., masked or in clear text); how long they will be stored; and how deactivated, disabled, and deleted identities will be stored.

3.5.7 Reporting

Different types of reports need to be created and used within the provisioning process. Many of the reports that are typically created are used for operational purposes, such as reports of system performance activities, tasks and queue management functions, and reconciliation events.

Audit reports include those that describe:

- Lists of identities and their associated access.
- The person approving access for specific information.
- The management of group and supervisory accounts.
- The number of users accessing a particular application or information resource.

Additionally, the processes and supporting systems should be able to provide reports that detail access approvals and reviews, because these are the areas of frequent weakness that are uncovered when auditing an organization's identity and access management process.

3.6 Enforcement Process

3.6.1 Authentication and Authorization

The enforcement of identities with their corresponding access rights occurs during the user's login to the application, as demonstrated in Figure 3. During login, the application performs a check to validate the user's identity. This process is called authentication and can take several forms. For instance, systems can require authentication by using a specific user characteristic (e.g., fingerprint ID or voice recognition), something the user has (e.g., smart card, badge, or key fob), or something the user knows (e.g., password or passphrase).

Once the identity is recognized and validated, the application will authorize the user to perform functions in the application based on the access rights associated with the user identity. Authorization of the user identity should be based on the access rights granted to the user during the provisioning process. Often, the authorization of a user identity may not correlate with the access rights that were intended to be granted to the user during the provisioning process. As a result, the monitoring and verification of access rights are important parts of the IAM process.

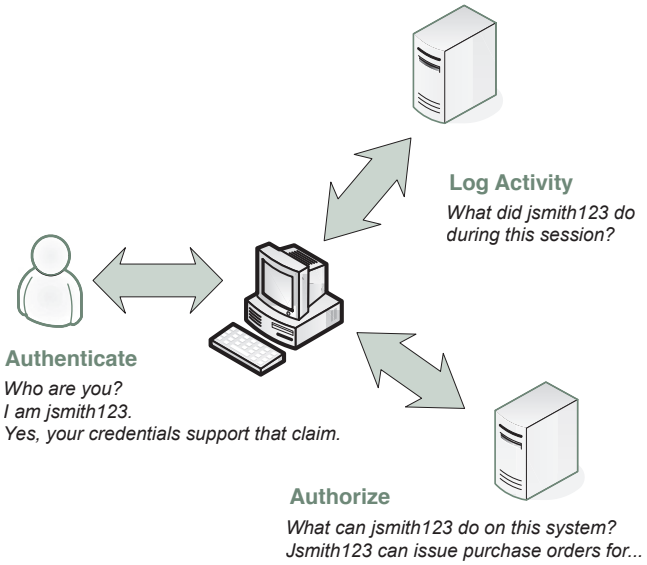

Figure 3. Enforcement of user access rights

3.6.2 Logging

Logging user identities, their access rights, and the functions they perform in the application provides the organization with a means to examine several items:

- Are user identities and their access rights in compliance with the access rights approved for the user identity?
- Are user identities and their access rights misaligned with the access rights necessary for the user identity to perform its functional responsibilities?
- Are user identities performing all of the functions granted to them through the provisioning process?
- Are user identities making password change requests on a frequent basis?
- Are user identities accessing or attempting to access applications outside normal business hours?
- Are there unauthorized attempts to perform certain functions by registered or unregistered users?

3.7 Use of Technology in IAM

3.7.1 What Types of Technology Exist?

When administering IAM activities, the majority of provisioning and enforcement processes can be automated through the use of IAM application software tools. These tools range

from applications that can be installed and used easily by organizations with small IT departments (e.g., less than 10 individuals) to applications that require customization for use by organizations with large or global IT departments.

3.7.2 Pros and Cons of Technology Use

While the use of technology certainly facilitates IAM, there are advantages and disadvantages to its use. Advantages include:

- Faster response times.
- Easily retrievable evidence of activities.
- Automated workflows for approvals and communication.
- Better management of large data volumes.
- Ability to centrally administer and monitor systems.

Disadvantages include:

- Lack of ownership.
- Lack of understanding of how to use the tools.
- Tools that may not be suited to the organization's size or complexity.

3.7.3 How Is the Technology Used?

The use of technology during the IAM process can be used to replace manual activities or to bolster the lack of some IAM activities. Business management needs to understand the technology being used and why it is used, while IT should install and maintain the tools to support business needs.

Tools can be used to perform any of the following activities:

- Generate access request forms.
- Route access request forms to approvers.
- Perform a preliminary segregation of duties conflict review.
- Communicate the creation, change, and termination of identities.
- Perform authentication and authorization of identities to applications.
- Generate logs of identities and their use.
- Generate passwords.

3.7.4 Additional Concepts

Single Sign-on

There are many ways to perform authentication for an identity within an IAM system. Single sign-on is one automated means of authenticating an identity to all IT resources to which the identity has been granted access rights, without requiring the identity to provide more than one series of authenticating factors (i.e., a user ID and password).

Remote Sign-on

In many organizations, identities, particularly human ones, are granted access rights to authenticate themselves to the IT resources from outside the organization. This type of remote access and authentication can occur in many ways, some of which are more secure than others. Examples of these mechanisms are:

- Virtual private networks, which are connections of networked devices between the organization's offices and the remote identity's site.
- Web portals, which are connections through an Internet-based interface with the organization's offices.
- Dial-up modems, which are connections between the identity's site and the organization's site that use ordinary telephone lines similar to placing a voice telephone call.

These remote connection types each have their own inherent advantages and disadvantages. For instance, access through a Web portal is the most universal in that it allows users to gain system access from nearly any system that has Internet access, yet it also puts proprietary or confidential information at risk of being compromised by the uncontrolled system on which the Web browser is located. Dial-up modems provide somewhat more secure, direct connections back to the internal network but with substantially slower performance than other connection options that use high-speed Internet connections. These are just two examples of the many factors that need to be evaluated when determining which users should be allowed to remotely connect to the IT environment and through what methods.

4. The Role of Internal Auditors

Internal auditors play an important role in helping organizations to develop effective IAM processes and monitor their implementation. Prior to conducting an IAM audit, auditors need to understand the organization's existing IAM structure, such as the company's business architecture and IAM policies, as well as the laws, regulations, and mandates for which compliance is necessary. When conducting the audit, internal auditors need to document the organization's identity and entitlement processes — as well as the repositories and the life cycle components for each — and evaluate existing IAM activity controls.

4.1 Current IAM Processes

The first step in the IAM process is to determine whether the company has an IAM program. This can be determined by asking the following questions:

- Are there policies in place for managing and administering user identities and access activities?
- Is there a strategy in place for addressing the risks associated with the IAM process?
- Is there a reference model the organization can use during the administration process?

When answering these questions, it is important to identify whether documentation already exists that addresses these issues to some degree.

In addition, when assessing a company's IAM posture, internal auditors need to identify certain key elements. The figure below shows that these elements are not entirely centered in technology but include:

- Aligning business and management units.
- Understanding existing laws and regulations.
- Establishing budgets.
- Developing achievable implementation plans.
- Defining how technology can enable a more effective control environment.

4.1.1 Business Architecture

The IAM business architecture refers to the procedures and workflow logic that are implemented in conjunction with an IAM software product. Defining and documenting this architecture is a critical step toward managing current and future business risks. As shown in Figure 4, IAM is not strictly about the use of technical tools that enforce rules. Rather, it is process-oriented and varies substantially from one organization to the next. For instance, as with any business process, automated and manual controls can be used simultaneously. As a result, it is important that the organization understands the controls involved in the management of identity and access.

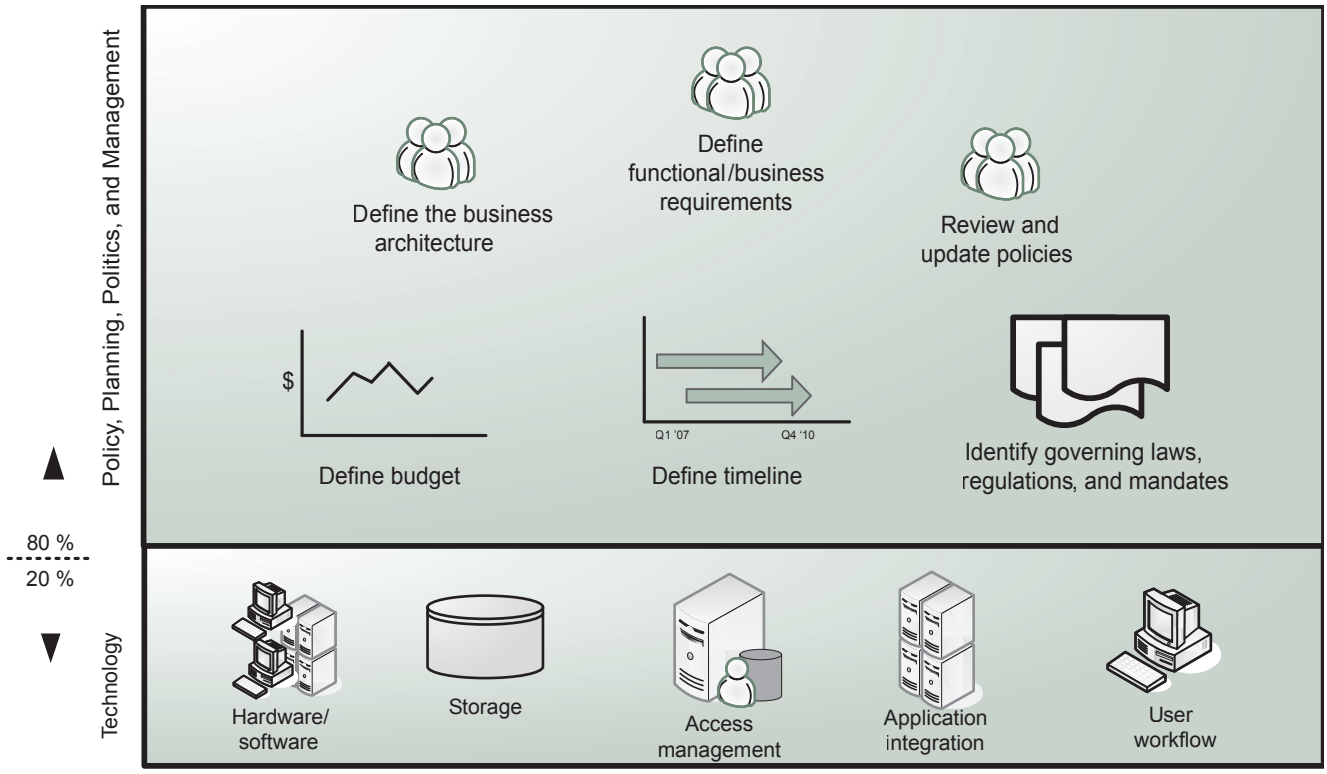

Figure 4. Process-oriented nature of IAM

Additionally, it is critical that the organization understands the roles and responsibilities of the individuals responsible for managing the control environment and maintaining the controls. Because many controls are automated or perform IT functions, management often assumes they are the responsibility of the IT department. However, business managers and data owners should be held responsible for the approval process.

Equally important is the commitment of senior management, in particular their understanding that IAM requires business leadership involvement to appropriately support companywide processes. For instance, if IAM is not given appropriate attention by senior management, the tone of the organization may not support IAM's importance.

4.1.2 Policies

Once the business architecture is documented or at least understood within the organization, existing policies and procedures that support this architecture and govern access management need to be reviewed. While these policies are often of a high level and may describe an organization's commitment to securely managing information, it is equally important for standards, procedures, rules, and guidelines to support each policy. This set of documentation is often referred to as the corporate policy framework.

In addition, although the vernacular and type of documentation will be unique for each company, it is important that the policy framework provides sufficient information to all employees about how user identities and access rights are to be managed, reviewed, and approved. Furthermore, the policy framework needs to explain how new business processes, applications, systems, and data repositories can be configured to align with the policy framework, as well as to ensure the new policies do not expose the organization to excessive risk.

4.1.3 Laws, Regulations, and Mandates

It is important for the organization to maintain operational efficiency and to make sure appropriate processes are implemented that enable the business to comply with different national and local laws, regulations, and mandates. Simply understanding these laws and regulations is not enough — organizations need to determine how they apply to IAM processes as well.

In many cases, the types of data that can be collected and transferred across country borders are tightly defined. For instance, countries with data protection laws that must comply with the Directive on Data Protection may limit the kinds of employee information that can be transmitted to systems and administrators outside the user's home country. However, because this personal information may be needed to perform entitlement reviews that grant users access to systems hosted in other countries, legal procedures must be in place to respond to this and similar situations. As a result, when auditing the policy framework governing the organization's handling of personal information, a review process must be in place to determine if applicable laws are addressed properly.

4.1.4 Budget

Funding for IAM initiatives needs to address the implementation of new procedures and any supporting technologies, as well as ongoing operations based on new IAM processes. Significant time and funding may be required to bring about organizational change and implement any technology tools that support IAM. This funding can include hardware, software, and consultants or contractors to implement the technology. Once the technology has been deployed, ongoing funding is necessary for any license fees and internal or external support staff. Depending on the organization's budget cycle, a business case for IAM may need to be developed and introduced into the annual budget process.

4.1.5 Timeline

If there is an IAM program in place or under way, there should be an evaluation of its implementation timeline and alignment with the organization's program management reporting needs. If specific reporting requirements need to be met, it is important for these dates to be communicated and managed jointly by the IAM program and other program management offices. Additionally, any complex program is likely to encounter timeline-related issues. Reviewing these programs and their ability to manage schedule changes successfully enables the audit team to determine the likelihood that the project will successfully meet future target dates and milestones.

4.1.6 Business Requirements

Whether there is a formal IAM program in place, it is still important that all systems have the ability to meet business performance requirements. If there is a program in place, a straightforward process of determining whether business stakeholder requirements were collected and reviewed needs to be operating before beginning the program's implementation. Depending on the program's current stage, the organization should be able to review whether existing systems provide the functionality required for the IAM program to operate effectively. If a formal IAM program is not in place, this may be more difficult. Business requirements may not be well documented or well known to the personnel managing the IT environment.

With the advent of Sarbanes-Oxley and similar regulations around the world, many organizations have instituted tighter controls over access administration processes. As a result, there should be guidance available within the organization regarding what is required to meet any regulatory requirements. Ultimately, all requirements should include the ability to answer these questions:

- Who has logical access to information?

- Is the level of access appropriate?
- Who approved the access?

4.2 Auditing IAM

Whether there is a defined program in place or not, internal auditors need to examine the identity and access management processes that exist within the organization.

4.2.1 Evaluation of IAM

Before developing an IAM audit approach or assisting with the creation of IAM processes, any existing identity management policies and procedures should be reviewed. Once current processes are identified, internal auditors can assist management by conducting a risk assessment that will enable the organization to develop an effective identity management process.

In addition to conducting a risk assessment, internal auditors can assist management or the identity management team in determining where new or additional team members should come from within the organization. Internal auditors can be valuable team members in this respect because they have visibility into all levels of the organization and understand what areas need to have a better identity management focus.

Document Identities

As part of the process, auditors need to clearly identify the different user identities that exist within the organization. (Refer to page 6 for a list of identity types.) Within each category of users, and in particular across complex organizations, several of these groups may have subgroups. Those most likely to have multiple subgroups include vendors and batch accounts.

Define Identity Life Cycle Components

Identity life cycle components include provisioning, administration, and enforcement. To define identity life cycle components, auditors need to determine the process, controls, and documentation that relate to the provisioning process. For example, if processes are manual, what orientation or training have administrators received? If processes are automated, is feedback generated to identify whether each process is working?

Determine Controls Within the Identity Life Cycle Process

As with any process, it is critical to identify the controls that affect it. Within the identity life cycle process, several key control areas exist that need to be reviewed. Controls can include approval processes for creating identities, access revocation processes, entitlement reviews, and access logging.

Before an identity is created, someone in the organization must approve it. For instance, a manager is likely to approve the hiring of a new employee. This hiring manager will work with human resources to help establish the person's identity in the system. This process typically includes collecting various pieces of personal information, determining whether the person has previously worked for the company, and eventually creating computer accounts for the person. Each step in this process needs to be reviewed to determine that there are appropriate controls throughout the identity life cycle, since the creation of identities must be controlled to prevent the introduction of unknown users into the environment.

Furthermore, the organization needs to properly deactivate or remove user identities that are no longer needed. Hence, policies need to clearly identify what needs to happen when people leave the organization. Reviews also need to be conducted to confirm that the appropriate action took place.

Determine Identity Repositories

To identify repositories, auditors need to determine where information about the identities is stored. This will typically include areas such as human resources, contractor database repositories, outsourced service provider databases, and external sales force databases.

For nonperson accounts, including system accounts, the information about how they are created, who has access to them, and what information about them is stored and maintained may be more difficult to document. Regardless, there should be a methodology in place for documenting the account types that are in use.

Document Controls for Identity Repositories

Once identity repositories are identified, the controls used to protect the data residing in the repositories need to be evaluated. This task will require several detailed reviews encompassing multiple controls. However, the reviews can be conducted like more traditional system, database, and application reviews. For instance:

- Are the machines that are storing the information secured?
- By what standards are they secured?
- Does the organization maintain standards on how to manage and operate these systems?
- Are the systems subject to the same standards as financial applications in general?
- Is access to the IAM systems, tools, and data repositories managed through the IAM system or through other means?

4.2.2 Evaluating Entitlement Management

Document Entitlements

Effective entitlement management processes necessitate documentation of entitlements that are granted to users of platforms, applications, and roles within applications, among others. As part of their role, auditors need to determine how entitlements are grouped together and what permissions

users, IT devices, service accounts, machine accounts, and batch accounts have.

Document Entitlement Life Cycle

Auditors need to determine and document any differences between the entitlement life cycle and the identity life cycle. Typically, the following major steps need to be identified in some form: entitlement creation, entitlement assignment, and entitlement removal.

In addition, auditors should keep in mind that large IAM programs may have processes established for creating new entitlements, grouping them together, and assigning them to either people or roles within the organization, while smaller organizations may use paper forms or spreadsheets to request and track access. Regardless of the method used, someone in the organization needs to approve access and make sure that access is granted on the system or application.

Determine Entitlement Life Cycle Controls

Access approval is one of the key controls within the entitlement management life cycle. This process needs to be considered carefully based on the nature of the organization. For instance, in smaller companies, granting access rights is frequently a straightforward decision. In larger organizations, however, it can be difficult to determine what access a person really needs to do his or her job. Furthermore, due to the complex reporting and management structure of many organizations, it may be hard for the designated approver to know the kind of access a person requires to perform a particular job function. Finally, controls need to be in place to ensure that systems are configured only after an appropriate approval is received.

Determine Entitlement Repositories

Entitlement repositories have a variety of enforcement mechanisms that need to be configured appropriately. To this end, many applications are capable of independently managing entitlements. This activity frequently includes performance of authentication and authorization functions. For example, applications may leverage a central authentication mechanism, such as a directory, or a central authorization mechanism, such as a portal or Web access management technology.

Many business processes depend on multiple applications and use multiple mechanisms for authentication and authorization enforcement. Regardless of which entitlement mechanism is used, auditors need to identify where the entitlement information is stored and how the entitlement information is managed.

Document Controls for Entitlement Repositories

The most important aspect that must be reviewed when documenting controls for entitlement repositories is whether the audited system contains the appropriate entitlements. For instance, auditors need to determine whether the entitlement repository accurately reflects the entitlements that are already in place. Frequently, there will be discrepancies between what is and what should be. Thus, determining where the weaknesses occurred can be challenging.

As with the identity repository information, all standard systems, databases, and application security standards need to be reviewed. Reviews of machine configurations should be conducted like any other configuration review, just as in the review of controls for identity repositories.

Identify How Reconciliation and Oversight Are Performed

The primary function of reconciliation is to verify that actual access aligns with approved access, as previously described. Many organizations have implemented specific processes for access review and reconciliation. The following three questions address several key elements within the process that should be reviewed:

1) Does repeatable and reliable reconciliation occur?

Auditors should review performance of reconciliation processes to determine if they are sustainable and repeatable. In addition, auditors should review these processes to determine their reliability — that is, is the process actually generating measurable improvement in the state of logical access control?

Simply reviewing the logical access and stating that it is appropriate is not enough. Many large organizations have encountered the "rubber stamp" review, in which the person responsible for performing the review stamps an approval on the entitlement report as a result of the person's inability to deal with the amount of users he or she is responsible for reviewing.

Because the review process could be thought of as a form of identification validation, the person performing the review should have some knowledge of the person for whom they are vouching (i.e., to state that an individual needs to have access to an application). If the process is such that the individuals validating access cannot possibly know all the users, the process needs to be made more effective. One possibility in this situation is to have lower-level managers conduct the reviews of their direct reports, rather than having a more senior individual review those with whom he or she rarely interacts.

2) How often do reconciliations occur?

Many organizations perform reconciliation reviews twice a year. However, once automation is involved, the process could be performed almost daily with any exceptions being automatically repaired or reported to the individuals responsible for managing access.

3) How are reconciliations handled?

To answer this question, auditors could ask the following:

- What happens when a reconciliation event occurs (i.e, what happens when what is does not match what should be)?
- Is the event simply logged for later review?
- Do the systems automatically reconfigure to align with what should be?
- What steps are taken to identify the root cause of the problem?
- Is the event only a technology problem or did someone make an unauthorized change to a system?

Appendix A: IAM Review Checklist

When auditing identity and access management (IAM), breaking down the information into three topic areas — administration, provisioning, and enforcement — allows a full review of the environment while enabling certain key questions to be answered. The following checklist is a high-level overview and is not intended to be a comprehensive audit program or address all IAM-related risks.

Topic areas:

- **Administration** — What is in place to develop and maintain an appropriate IAM strategy, policies, procedures, and ongoing operations?
- **Provisioning** — How is access granted, monitored, and removed within the environment?
- **Enforcement** — Are appropriate measures in place to deter, prevent, and detect attempts at evading IAM processes?

Audit Question/Topic	Status
1.1 Is there an IAM strategy in place? A critical element for an effective IAM process is the presence of a consistent approach to manage the supporting information technology (IT) infrastructure. Having a cohesive strategy across the organization will enable all departments to manage people, their identities, and the access they need using similar processes, if not necessarily with the same technology. • Inquire about current IAM strategies in the organization. • If they exist, determine how and by whom they are managed.	
1.2 Are the risks associated with the IAM process well understood by management and other relevant individuals? Are the risks addressed by the strategy? Simply having a strategy does not ensure it covers all the risks that IAM may present. It is important that the strategy contains elements that identify all relevant risks. • Determine whether a risk assessment of esatablished IAM processes was conducted. • Determine how risks are identified and addressed.	
1.3 Is the organization creating or changing an IAM process only to satisfy regulatory concerns? It is critical that IAM processes are integrated with broader business issues and strategies. There are numerous benefits to having a robust IAM environment, such as having a better internal control environment. • Determine the needs of the organization with respect to IAM. • Determine whether the IAM processes extend into the organizaton or just meet an external third-party requirement.	
1.4 Are the regulations governing the organization well understood? New regulations are being created, and for large multinational organizations, it can be difficult to identify all of the regulatory requirements with which the organization must comply. • How does the organization determine the regulatory requirements it must meet? • How does the organization remain current with these regulations? • How does the organization capture, store, and retrieve this information?	

Audit Question/Topic	Status
1.5 Are there defined methods to appropriately account for issues related to segregation of duties? While many areas of the business have defined rules to manage issues with segregation of duties, these typically are not well documented or understood. The main question to ask is whether or not managers and other personnel responsible for approving access are capable of recognizing when a segregation of duties weakness occurs. • Are segregation of duty conflicts identified within IAM processes? • How are these conflicts dealt with? Who deals with them? • Are there mechanisms in place to capture or identify these conflicts before access is granted?	
1.6 Is the IAM environment centralized or distributed appropriately to reflect the structure of the organization? An ideal technical situation would be to have a single software solution with consistent processes clearly documented and managed through a single implementation tool. However, due to the challenges associated with legacy system integration and the modification of processes used to grant approvals, these technologies have not lived up to their potential. • If multiple IAM solutions exist, how are they managed to identify, prevent, or detect unauthorized or unnecessary permissions granted to users?	
1.7 How are password policies established, and are they sufficient for the organization? Policies that govern IAM processes are critical components of any effective solution. Therefore, it is important to understand how the policies are established, how they are communicated, and how the technology elements of the environment support their compliance. • What password parameters have been established for companywide applications? • Are they consistently applied? • How are changes to these parameters controlled?	

Audit Question/Topic	Status
2.1 Does the organization have consistent processes for managing system access? Several provisioning aspects elicit questions. These questions, which need to be asked and ultimately answered, relate to individuals' knowledge of processes, any documentation produced, and adherence to specified processes. • Determine whether IAM-related policies and procedures exist in the organization. • Determine whether the policies and procedures have been communicated to the appropriate individuals in the organization.	
2.2 Can auditors uniquely identify the individuals who are granted access to the organization's systems based on the sign-on credentials they are assigned? A critical element within the provisioning process is the ability to successfully identify the people for whom access is managed. • Are unique identifiers in place for users of IT resources? • How are these identifiers tracked and recorded?	
2.3 Is employee productivity degraded because it is too difficult to gain and maintain system access? As noted, key drivers of IAM system adoption are the regulatory requirements that call for better controls. There are clear benefits to implementing these types of systems. However, the manual processes that typically are employed to manage access are incapable of providing ready access to these systems. • How is the IAM process managed in the organization? • Are there benefits to having part of the IAM process become self-sufficient for users (e.g., password resets, use of a help desk application versus a call-in number)?	
2.4 Who should approve access for a user in the environment? This is an important question that must be answered. Another is whether there should be multiple people involved in the approval granting process. • Determine the methods used to approve user access requests. • Determine whether the approval rests with the business unit or IT department. • Determine how segregation of duty conflicts are approved.	
2.5 Can the organization demonstrate that only appropriate people have access to information? This is a critical question for an auditor to answer. However, demonstrating that the organization has control of user access can be difficult. • How often does the organization review the access granted to its users? • If a review is performed, how is inappropriate access identified, logged, and addressed?	

Audit Question/Topic	Status
2.6 Are there appropriate controls in place to prevent people from adding access to systems and applications outside the approved process? Having a process in place to manage identities and access to systems and applications sounds like an ideal situation. However, how can organizations ensure that people are not circumventing the process and adding their own accounts or the accounts of others without proper authorization or adherence to defined processes? • Determine who in the organization has the ability to add, modify, or delete users from the applications used in the environment. • Determine whether there is a periodic review of users that traces their access permissions to access request forms.	
2.7 When people leave the organization, does it identify what system access they have and revoke it in a timely manner? One of the main findings in IAM audits is persistence of accounts that retain access long after the account owners leave the organization. The challenge relates to identifying all access associated with a specific user. • Does the organization have a process in place to deactivate or delete user access permissions when they are no longer needed? • How does the organization ensure that all account names associated with a particular individual were deactivated or deleted?	
2.8 What does the organization do with respect to nonperson accounts? Nonperson accounts are challenging for several reasons, not the least of which is determining the controls associated with these types of accounts. • What functions does the account perform? • Does the account need to exist and be active? • Who has access to the account? • Is there a shared password for the account? • How many people know the password? • How do you maintain accountability for actions performed by the account?	
2.9 What does the organization do with respect to privileged accounts? Privileged accounts provide a unique set of challenges. These accounts are required to manage the environment and to provide consistent, timely, and high-quality support. However, privileged accounts also have the capability to circumvent many of the controls that are put in place to manage access for typical accounts. • Determine the individuals in the organization who possess privileged access permissions to the applications used in the organization. • How are the privileged access permissions requested, approved, and granted to these individuals? • How often are granted access permissions reviewed?	

Audit Question/Topic	Status
3.1 How strong are the controls in place to prevent people from bypassing authentication or authorization controls? One of the pressing challenges for applications is the enforcement of access and how the individual applications manage authentication and authorization. • Determine the means of authentication in use for existing applications. • Determine whether the means of authentication present opportunities for users to circumvent the authentication process (e.g., weak or saved passwords).	
3.2 Is there a uniform approach for applications to enforce access? IT leadership must define how this issue will be managed and how systems will enforce the decisions that are made. • Are passwords synchronized among the applications used in the organization? • How are synchronization mechanisms managed, if they are used at all? • Without synchronization, what mechanisms are in place to prevent users from accessing applications to which they are not granted access?	
3.3 How is information logged, collected, and reviewed? It is important to understand what types of events are logged, where they are captured, and how frequently they are reviewed. • Determine whether the organization uses event logging with respect to IAM. • If event logs are used, determine when and how they are reviewed. • If logs are reviewed and discrepancies are discovered, how are these items resolved?	

Appendix B: Additional Information

Additional information can be obtained from the following external resources:

- Canaudit, www.canaudit.com.
- *Chief Information Officer* (CIO) magazine, www.cio.com.
- *Chief Security Officer* (CSO) magazine, www.csoonline.com.
- Control Objectives for Information and related Technology (CobiT), www.isaca.org/cobit.
- Federal Financial Institutions Examination Council (FFIEC), www.ffiec.gov.
- IBM Corp., www.ibm.com/software/tivoli.
- ISACA, www.isaca.org.
- The Institute of Internal Auditors, www.theiia.org.
- Microsoft Corp., www.microsoft.com/technet/security/guidance/identitymanagement.
- Oracle, www.oracle.com/products/middleware/identity-management/identity-management.html.
- Public Company Accounting Oversight Board (PCAOB), www.pcaobus.org.
- SysAdmin, Audit, Network, Security (SANS) Institute, www.sans.org.

Glossary

Access(es): The right or permission that is granted to an identity. These informational access rights can be granted to allow users to perform transactional functions at various levels.

Authentication: A process for attempting to verify an identity against values in an identity repository. It is a way to validate that users are who they claim to be.

Authorization: A process for determining what types of activities are permitted. Ordinarily, once a user has been authenticated, he or she may be authorized to perform different types of activity or granted certain access rights.

Entitlement: Access to specific functionality in a system or application that is granted to a specific user. Most individuals in an organization have multiple entitlements granted for access to multiple systems.

Identity: A unique sequence or set of characteristics that uniquely identifies an individual.

Identity and access management (IAM) repository: A data storage facility that houses all of the current and historical data for the IAM system.

IAM system: A system consisting of one or more subsystems and components that facilitates the establishment, management, and revocation of identities and accesses to resources.

Life cycle event: An event that occurs during a user's life cycle, which may trigger an IAM system process (e.g., termination or transfer).

Offboarding: The process through which an individual leaves a role as an employee or contractor for the organization, returns any physical assets assigned to him or her, has physical access rights revoked, and has logical (i.e., application and system) access rights terminated.

Onboarding: The process for identifying an individual to bring into an organization as an employee or contractor; providing the individual with the tools necessary to perform his or her job; and creating an identity, accounts, and access appropriate for his or her duties.

Provisioning: The process used to create identity, associate identities with access, and configure the systems appropriately.

Resource: An object in the IAM system that can be requested by a user, including an application, a component of the technology infrastructure (e.g., system), or a specific access or entitlement (e.g., group or profile).

Security model: A security rule within an application that connects the lowest level of security (i.e., security setting) to the highest level of security (i.e., security groups). Security groups are assigned to users.

Segregation of duties: A control mechanism whereby a process is broken into its constituent components and the responsibility for executing each component is divided among different individuals. Segregation of duties segments the process so that no individual has an excessive ability to execute transactions or unilaterally cover irregularities without detection.

Sensitive entitlement: A resource or access identified to potentially present a level of security risk to the organization if or when provisioned. Examples include special authorities, domain administrator groups, and access to the root account.

Transfer: A life cycle event whereby a user changes job responsibilities or functions.

User ID: An identifier or login ID on a specific resource used to manage access to that resource.

About the Authors

Frank Bresz, CISSP
Frank Bresz is an executive director in the Ernst & Young financial services office, where he is responsible for information systems security strategy and strategic program operations. Bresz has worked with clients to develop their information security programs and has focused on aligning the security program's vision with existing and pending regulations.

Bresz has more than 22 years of experience in information security and data center operations and has a strong background in developing large identity and access management (IAM) programs as part of broader information security initiatives. Prior to working with Ernst & Young, he was responsible for information technology (IT) management for 10 years and has worked extensively with Sybase in developing Web-based applications.

Bresz received his bachelor's degree in computer science from the University of Pittsburgh. He is a certified information systems security professional.

Sajay Rai, CISSP, CISM
Sajay Rai is a partner in Ernst & Young's risk advisory services practice. He has more than 30 years of experience in IT, specifically in the information security, business continuity, and risk management disciplines. Rai previously worked with IBM as a managing director of the national business continuity and contingency consulting practice. He was instrumental in starting the company's information security consulting practice and managing its IT consulting practice in Latin America.

Rai co-authored a recently published book, *Defending the Digital Frontier: A Security Agenda*, which guides business and IT executives on how to develop an effective and efficient information security program. He has been named in the *Crain's Cleveland Business Who's Who in Technology*.

Rai has a master's degree in information management from Washington University and a bachelor's degree in computer science from Fontbonne College. He is a certified information systems security professional and a certified information security manager.

Tim Renshaw, CISSP
Tim Renshaw is a senior advisor in the Ernst & Young financial services office. He has experience in program management and IT within the financial services and pharmaceutical industries. Renshaw has developed IAM implementation strategies for several global financial services institutions and has worked with clients in the financial services industry to develop risk self-assessment programs and information security strategic plans. In addition, he has established and operated IT program management offices, performed independent reviews of enterprisewide technology implementation projects, and supported business process re-engineering initiatives.

Renshaw received a bachelor's degree in information systems and in economics from Carnegie Mellon University. He is a certified information systems security professional.

Jeffrey Rozek, CISSP
Jeffrey Rozek is a senior manager in Ernst & Young's global risk advisory services practice, where he specifically focuses on information security. He has nearly 15 years of information systems and security experience in the financial services, telecommunications, manufacturing, and utilities industries. Rozek has led numerous security projects, including large, multinational, and multi-language implementations, and has concentrated on providing access control, authentication, and authorization solutions. He has worked with a number of Fortune 100 companies in assessing and developing their overall security and risk frameworks and maturity models, and also has assisted clients in architecting, designing, and deploying technical security architectures.

Rozek has a bachelor's degree in accounting from John Carroll University and is a certified information systems security professional.

Torpey White, CPA, CISA

Torpey White is a director in Goldenberg Rosenthal's management consulting practice where he provides consulting advice and attest services to Fortune 1000, middle-market, and nonprofit organizations. White is experienced in internal control assessments, operational reviews, Statement on Auditing Standards No. 70 examinations, U.S. Sarbanes-Oxley Act of 2002 Section 404 project administration, internal auditing, accounting assistance, financial reporting and analysis, business process analysis, and business process documentation and reengineering.

White has 20 years of experience and has worked for organizations in various industries, including those in the software development, utilities, automobile dealers and auctions, horse racing, health-care, nonprofit, and light manufacturing sectors. He also performs internal audit plan development and management, financial systems implementations, budgeting and forecasting, legacy system support, acquisition support, and special project implementations.

White received bachelor degrees in accounting and finance from LaSalle University. He is a certified public accountant and a certified information systems auditor.

Reviewers

The IIA thanks the following individuals and organizations who provided valuable comments and added great value to this guide:

- Ken Askelson, JCPenney, USA.
- Lily Bi, The IIA.
- Lawrence P. Brown, The Options Clearing Corp., USA.
- Tim Carless, Chrysler Financial, USA.
- Christopher Fox, ASA, eDelta, New York, USA.
- Nelson Gibbs, Deloitte & Touché LLP, USA.
- Steve Hunt, Enterprise Controls Consulting LP, USA.
- Stuart McCubbrey, General Motors Corp., USA.
- Heriot Prentice, The IIA.
- James M. Reinhard, Simon Property Group Inc., USA.
- Paula Stockwell, IBM Corp., USA.
- Jay R. Taylor, General Motors Corp., USA.
- Hajime Yoshitake, Nihon Unisys Ltd., Japan.

The Ernst & Young Point of View on Key Issues

Ernst & Young

Quality In Everything We Do

For automotive companies, every day is a race to pull ahead of the competition by improving global operations, optimizing investments, and mitigating financial risk—all while keeping an eye towards the key business issues on the horizon.

Dealing with Industry Consolidation, Restructuring, and Business Spin-offs

The industry, especially in the US market, is in transition. Automotive industry consolidation, restructurings and spin-offs will create significant business change management and other transition issues will bring about new risks throughout the automotive value chain. The emergence of new market leaders in the vehicle manufacturer and supplier segments will lead to new challenges for established vehicle manufacturers and suppliers related to customer, vehicle platform and product mix.

Solving Operating and Profitability Problems in Key Markets, Especially North America

Globally, the sector is growing. However, in the largest market in the US, many vehicle manufacturers and suppliers are experiencing poor operating performance, poor profitability, and increasing financial and bankruptcy risk. These profitability challenges have led to on-going changes in organization and operating structures, creating significant process improvement and cost reduction needs for these companies.

Improving Compliance Risk Management Activities

Compliance and risk management is a continuing imperative in the automotive supplier community, particularly with the increase in globalization. Improving compliance-related activities, including better enterprise risk management, improving compliance efficiency, and reducing the costs of compliance are continuing needs of automotive companies.

Developing Strategy and Managing Operations in Emerging Growth Markets

Automotive companies are in the process of developing, refining or managing strategies for emerging markets, especially in China, Mexico, Brazil, India, and Eastern Europe. Strategies to monitor risk in these areas create significant on-going challenges for companies to manage.

Developing Strategies to Retain Knowledge and Key Competencies as a Result of the Automotive Industry Transition

As the number of workers are displaced in the industry and operations continue to globalize, the need to retain knowledge regarding key processes including finance and accounting, engineering, procurement, manufacturing is increasing. Developing strategies to address this outgoing knowledge is a significant challenge for companies.

Ernst & Young

www.ey.com

© 2007 EYGM Limited.
All Rights Reserved.

EYG - ED0007

Creating Innovative Solutions to Address the Climate Change Impact on Product Strategy

As mounting scientific evidence indicates the earth's climate is currently warming, more companies and organizations are taking action to reduce their impact. New pieces of legislation to reduce emissions and greenhouse gas are being introduced with growing frequency, many of them with different incentive packages and time frames for compliance.

The Ernst & Young Global Automotive Center can help automotive companies address industry challenges by drawing on the insights and practices of an international network of member firms. The Center acts as the focal point for our automotive professionals, facilitating the collaboration and knowledge sharing required to develop approaches to complex industry issues. Ernst & Young is working to establish automotive centers in Detroit, Stuttgart, Beijing, and Tokyo—all of them linked and focused on the issues that are driving massive transition in the industry worldwide. Globally, the industry shows very significant growth, however, in key markets such as North America, the expansion is uneven and major transitions are under way.

About Ernst & Young
Ernst & Young, a global leader in professional services, is committed to restoring the public's trust in professional services firms and in the quality of financial reporting. Its 114,000 people in 140 countries pursue the highest levels of integrity, quality, and professionalism in providing a range of sophisticated services centered on our core competencies of auditing, accounting, tax, and transactions. Further information about Ernst & Young and its approach to a variety of business issues can be found at www.ey.com/perspectives. Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited does not provide services to clients.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

Your contact person at the Global Automotive Center:

Randy Miller
Automotive Global Markets Leader,
Risk Advisory Services Leader

Randall.Miller@ey.com

+1 313 628 8330

GTAG®

Identity and Access Management

Identity and access management (IAM) is a cross-functional process that helps organizations to manage who has access to what information over a period of time. This process is used to initiate, capture, record, and manage the user identities and related access permissions to the organization's proprietary information. Poor or loosely controlled IAM processes may lead to organizational regulatory noncompliance and an inability to determine whether company data is being misused.

Chief audit executives (CAEs) should be involved in the development of the organization's IAM strategy as well as evaluate the implementation of the strategy and effectiveness of companywide access controls. The purpose of this GTAG is to provide insight into what IAM means to an organization and to suggest internal audit areas for investigation. It can assist CAEs and other internal auditors to understand, analyze, and monitor their organization's IAM processes.

Visit www.theiia.org/guidance/technology/gtag/gtag9 to rate this GTAG or submit your comments.

Order Number: 1039
IIA Member US $25
Nonmember US $30
IIA Event US $22.50

ISBN 978-0-89413-617-7

9 780894 136177 53000

The Institute of Internal Auditors

www.theiia.org

07526