FASTPATH
now part of Delinea

Managing Identity and Access Controls Across Multiple Applications

FASTPATH
now part of Delinea

Table of Contents

With the rise of remote working, geographically distributed workforces, and the shift to the cloud, protecting identity and preventing fraud has never been more important. Employees need fast access to technology to be productive, but over-provisioning can result in organizations being exposed to serious risks. The growing severity and sophistication of cyberattacks mean enterprise leaders have a complex set of security and compliance needs. They must focus on safeguarding data and sensitive information, while at the same time enabling the organization to operate efficiently.

The Risks that Come with Business Transformation

While external events have changed the way we do business, many internal changes are taking place as well. New technologies bring about new capabilities, like process re-engineering and automation, making the organization more efficient. And new cloud platforms are providing universal access to applications that enable the mobile and remote workforce.

Strategic business practices, like mergers and acquisitions, have varied business environments as well. In the process of gaining a competitive advantage, these organizations might acquire an entirely separate IT infrastructure along with new risks and challenges to monitor, manage, and control.

All these developments have completely reshaped the way organizations are interfacing with their environments today. The velocity of change has increased. The threats are changing. The technologies are changing.

Therefore, it's vitally important to think about how the organization identifies, assesses, and responds to access risk across this varied and dynamic landscape.

Some of the questions to ask include: Who has access to our systems? Why are they accessing it? What can they do in that system? Are we vulnerable in any of those points?

Organizations should be aware of their risks and implement a risk management program to quantify and mitigate these risks:

- Be proactive to protect high-value assets.
- Increase visibility into key risk areas for informed decision-making.
- Implement a risk management plan with the agility to handle changing trends and landscapes and ensure efficiency/usability.

The Evolution of Business Application Landscape

As organizations have begun to move away from the traditional single business application database model toward best-of-breed applications, there has also been a shift towards using a mixture of cloud-based and on-premises applications from various vendors.

It is not uncommon to see an organization use their SAP S4 system or Oracle Cloud application to manage the centralized finance activities with additional applications running concurrently: Workday for HR functions; Salesforce for CRM; and perhaps additional applications, like Dynamics or NetSuite, which were acquired through mergers and acquisitions.

As more interconnected applications are introduced into the business environment, the challenge to monitor and manage access risk across the entire landscape becomes more complex.

For example, most organizations understand the potential Separation of Duties (SOD) risk involved when a single individual can create and process vendor invoices in addition to maintaining vendor master data.

But consider a situation where the user maintains vendors in a CRM system and then pays these vendors from the central finance system, or perhaps an HR representative maintains employees in an application like Workday and then processes payroll through the central finance system, like Oracle or Dynamics. These situations, which are becoming more the norm rather than the exception, demonstrate the need to assess security and access risk across various business applications, not just individual applications in isolation.

Knowing who has access to the various systems does not necessarily mean that you know what they are doing. Businesses need to also know:

- The securable objects accessible from each role
- Which user has been assigned to each role
- Cross-application risk presented by each user
- Which users no longer require certain access privileges

Fastpath helps organizations manage access and security risk concurrently across multiple business systems, providing an end-to-end view of their risk exposure and the tools to eliminate or mitigate those risks.

Managing Access Risk

As organizations introduce more applications across various platforms into their environment, they must accommodate new security models and objects, including separation of duties, conflict resets, security roles, and user provisioning processes. In addition, the regulatory landscape is changing. Regulations such as GDPR in Europe and CCPA in the States (among others) require organizations to secure customer data. It extends beyond just monitoring who has access to customer data, and organizations must also be aware of where that data resides. Organizations must have key controls in place where the information is maintained: at the application layer and database layer.

FASTPATH
now part of Delinea

The Evolving Business Application Security Landscape

Properly monitoring the risks within the business environment requires understanding the applications and how the applications themselves are evolving. Each release can introduce new components, securable objects, transaction codes, and security settings which can impact how users monitor and manage master data. The foundation of compliance is managing and monitoring access risk across an organization's risk universe, which may span across multiple applications. The separation of duties and sensitive access risk ruleset is the key framework for assessing risk. In addition, defined policies and procedures are critical to governing security and access risk.

Your ruleset should reflect your risk universe, including any cross-application risk that may be new to your organization.

Additional Vulnerabilities

It is important to highlight other components of an access risk management program that should be considered with the multi-application landscape, including security at the network, OS, client, database, and application layers. Below are examples of risks that should be managed in the business application landscape:

- System accounts often have default passwords out-of-the-box. If those passwords are not changed, malicious individuals can exploit that weakness and gain access to critical data in the environment.
- Unencrypted client-server and server-server communication protocols in business systems, such as APIs, make data traffic vulnerable to network sniffing, man-in-themiddle, and other attacks. Organizations should also monitor to make sure they are still in use, and if they are not, they should be decommissioned so they cannot be used later for an unintended purpose.
- Having extended delays in implementing critical security or

kernelpatches can expose the systems to vulnerabilities that are published and known by malicious hackers who can access the data and change it without going through the application itself.

Addressing Access Risk

When we start to think about access risk management, one of the first steps we should take is defining the enterprise's risk universe. Organizations must identify key stakeholders, such as business process leads or global process owners. Organizations might have one or multiple systems that are leveraged for critical business processes. Analyzing the end-to-end business process will ensure that the organization truly understands where the handshakes between multiple systems occur and that it addresses all the cross-system risks associated with that process. By gaining a thorough understanding of the organization's cross-platform risks associated with business processes, the internal and external audit staff can evaluate the risks, align them with the organization's risk and controls policies, and design rulesets to mitigate or remediate the risks.

SOD Management

Managing and monitoring access risk begins with defining a framework from the top down. Establishing clear roles and responsibilities for all stakeholders and defining the policies and procedures to maintain a compliant system are critical to the success of the overall program.

The policies and procedures should be comprehensive and consist of risk tolerance levels, remediation and mitigation strategies, provisioning processes, periodic reviews, approval processes, and much more. This is essentially the playbook for managing access risk.

The foundation of monitoring risk is the SOD and sensitive access ruleset. As highlighted above, this should represent the risk universe consisting of processes that operate within a single application or across multiple

applications. Fastpath's Access Control module identifies access in ERPs and other business software by user, role, and privilege and reports conflicts or risks associated with that access.

Emergency Access

One area of high-level risk is the need for emergency access—referred to variously as Firefighter Access, Emergency Access, Temporary Escalated Access, or Privileged Access Management (or PAM)—which involves granting someone elevated access privileges for a specified period. Elevated privileges are traditionally granted to IT to monitor sensitive access, perform break/fix duties, or even functional support. During the pandemic, there was an increase in use cases for businesses to obtain escalated access due to reduced workforces and colleagues out sick
or taking care of loved ones. The backup is granted elevated privileges until that person's colleague returns, mitigating the risk with approval processes and audit log monitoring. The organization must understand how the emergency access will be designed and provisioned and how to effectively manage the risk, starting with answers to some basic questions, such as:

- How should we be granting emergency access?
- Who should be approving that elevated access?
- What access should be given?
- Who should review and sign-off on the audit logs?

There might be times when emergency access needs to be cross-functional, or it might make sense to keep elevated access segregated between business functions, such as finance and the master data team.

Emergency access requests should be documented to provide an audit trail of the requests and approvals. Whenever emergency access is granted, the access must be de-provisioned after the emergency period has passed.

In addition, logs should be reviewed promptly to confirm that the activities during that elevated access are appropriate. If the activities were not appropriate, the team follows up to determine what those additional actions were and review them for any risk. Finally, any reviews should be documented, which will assist in future audits.

The Fastpath Identity module provides automated provisioning to business applications based on identity policies or rules and offers the flexibility to configure multiple approval scenarios including auto-approval, conditional, FCFS or appropriate reviewers. Additionally, Fastpath's dashboard feature provides real-time insight to the status of the certification process, further streamlining a traditionally manual process.

Access Certification

Access certification focuses on establishing procedures for reviewing user access assignments across a variety of systems and applications within the organization. Even if the separation of duties risk is not violated, it is still essential to ensure access appropriateness and that the principle of least privilege access is followed. Doing so can help alleviate any potential for SoD or sensitive access violations in the future. One of the first steps in defining access certification processes for an organization is making sure that all roles and access privileges are reviewed and documented by the process owners at regular intervals. Both internal and external auditors should approve the frequency of these certification reviews.

The Certification module in Fastpath can help build workflows based on business requirements, enforce timely certification reviews, and automate the review process for managers and business leads, significantly reducing the time of the process and reducing much of the manual effort.

User Provisioning

A compliant user provisioning process is paramount to an access management governance program. Even if all roles and users are clean of SoD and sensitive access risks, all the hard work becomes wasted effort if compliant user provisioning processes are not defined and followed. User provisioning processes are often manual when access management tools are not in place. Manual processes traditionally use a ticketing system but can also include emails, sticky notes, and even hallway conversations. Such manual processes can be time-consuming, prone to errors, and unreliable for audit purposes.

Provisioning and de-provisioning processes should be documented, auditable, and consist of preventative controls. Together, these processes function as the "gatekeeper" to prevent access risk from being introduced into the system. As such, it is essential to define the end-to-end process for users to request access, business process owners to approve that access, integrated access risk checks, and the workflow paths based on request components and criteria.

Fastpath's Identity module automates user provisioning. It provides auditable workflows, starting with the initial access request through the approval, provisioning, and if necessary, de-provisioning process. The Access Control module analyzes all requests, identifies any SoD conflicts present at the time of the user request, and allows for mitigation of any conflicts before the user is created.

Role Management

Security roles are the vehicles in which we deliver security authorizations to end-users. A framework must be established for maintaining the security architecture and key design principles, including:

- Ensuring all single roles are free of SOD and sensitive access conflicts
- Ensuring roles with access to view data are separated from roles with access to modify data to avoid introducing unnecessary risk

- Establishing a defined naming convention to easily identify the access being granted to the role to avoid inadvertently assigning more access than the role requires
- Developing and enforcing governance policies to ensure the role and access privilege guidelines are followed
- All roles are assessed for SoD and critical access risk before migrating through the landscape, establishing a clear ownership framework for role content and provisioning approvals.

The Fastpath Access Control module can be leveraged for what-if analysis or simulations to ensure security roles are designed without SOD or sensitive access risk. This, combined with periodic reviews such as role content and access certifications, further helps meet the organization's security compliance guidelines.

Sustaining into the Future

Access management governance is the overarching framework to achieving and maintaining a compliant landscape. This starts at the top with executive sponsorship and cascades down to all stakeholders within the organization. Policies and procedures are created to document the key components of each domain previously highlighted and other controls and governance principles. Other topic areas may include controls framework, periodic review requirements, policy and procedures change tracking/signoff, risk tolerance levels, and much more.

Much like your security architecture and design, the access management governance program should be scalable and updated frequently. Updates may be required based on transformation projects introducing new functionality and processes or even organizational changes. For example, suppose a new application is added to the environment. In that case, the ruleset should be updated to cover single-system and cross-system access risk, master data such as role owners should be defined, and role naming conventions should be updated.

One critical aspect is embracing technology to augment security and compliance activities. This can introduce additional detective and preventative control capabilities, streamline end-to-end processes, reduce human error, and provide overall visibility into managing access risk across the landscape.

Cross-application Risk Management: How Fastpath Can Help:

Fastpath is a cloud-based access orchestration that helps answer these critical questions:

- Who has access to our systems?
- What did they do with that access?
- Where is our organization vulnerable?
- Who can create a vendor and then pay that vendor with no oversight?
- Who has access to modify the chart of accounts, journal entries, or bank account data for vendors?
- Who is turning approvals on and off, or opening and closing periods?
- What data are the operating system administrators and database administrators changing?

The Fastpath platform offers a suite of applications to help manage SOD risks, automate user provisioning and track critical changes to the business systems. Most users will find the following product features useful:

- **Change Tracking**
  - Whether you leverage out-of-the-box templates or define the scope of the change tracking yourself, Fastpath's change tracking will identify who made the change and provide before & after values and other metadata to determine appropriateness. Integrations into common ITSM platforms allows you to close the loop by validating tickets and approvals where required.

- **Certifications**
  - No matter how effective preventative control of user access is, inappropriate access in key applications will happen. Fastpath helps you build a robust continuous monitoring program that detects issues quickly, reducing exposure time and eliminating issues. Certification campaigns can be set up with different targets and schedules to give you the most coverage possible.
- **Identity**
  - Whether you leverage out-of-the-box templates or define the scope of the change tracking yourself, Fastpath's change tracking will identify who made the change and provide before & after values and other metadata to determine appropriateness. Integrations into common ITSM platforms allows you to close the loop by validating tickets and approvals where required.

Fastpath also offers native integration with other GRC tools, including Workiva, ServiceNow, Coupa, Zendesk, and Jira, and comes with native, auditor-created rulesets for many business applications, making cross-platform rulesets easier to merge.

FASTPATH
now part of Delinea

About Fastpath

Fastpath is a leading provider of innovative Identity Governance and Administration (IGA) and Governance, Risk, andCompliance (GRC) solutions. We empower businesses to manage identity and access risks, ensuring robust security andregulatory compliance across multi-site, multi-application environments. Our easy to implement and easy to use, comprehensive platform enables companies to gain deep insights into identity and access risks, allowing them to take proactive measures to prevent fraud and protect their sensitive information and critical resources. Find out how we can help you make informed strategic decisions confidently, knowing your organization is fully secure and compliant, by visiting: www.gofastpath.com