Managing Risk & Discovering Value with Fastpath During an ERP Implementation or Upgrade

Chris Aramburu

FASTPATH

Table of Contents

The current ERP market has transformed significantly over the past several years. The software leaders in the space continue to reshape their ERP portfolios, release process-specific applications, introduce mobile capabilities, redesign the user experience (UX), and offer a variety of deployment options with cloud products. In parallel, integration technologies and standards facilitate the deployment of a variety of enterprise applications. Organizations now have the capability to leverage integration technologies to implement a "best in breed" or heterogenous architecture to best suit their needs. Through this approach, organizations can implement systems that reduce the total cost of ownership (TCO), enhance user experience, streamline business processes, obtain competitive advantages, and much more.

Organizations are responding to the efforts put forth by software vendors, whereas nearly 50% of companies are planning to or are already going through an ERP implementation or upgrade (according to g2.com). Selecting the ERP is just the first challenging step in a long journey. If you have ever been through an ERP implementation, you know this all too well. There is no shortage of pitfalls or mistakes to avoid when implementing your ERP system. Failing to include the Compliance team early on in your implementation efforts is a perfect example—and it can be a costly one.

Far too often the compliance team is left out, de-prioritized, or not even considered during the implementation until it is too late. This leads to costly mistakes or even prolonged risk exposure that could have been avoided from day one of the system being live. The words "compliance" and "reduce costs" are rarely discussed together; however, we see higher long-term costs for organizations that must go back and redesign or retrofit their solution with compliant controls and/or security architecture, leading to additional resource consumption and opportunity costs.

Security as a Cornerstone in an ERP Implementation

A "design-in" approach is a concept you might already be familiar with. This concept also applies to compliance within an ERP implementation or upgrade. By including your compliance team, you can design compliant processes integrated with configurable controls (e.g., tolerance levels, approval workflows, delegation of authority, etc.), develop compliant security models preventing segregation of duties (SoD) conflicts or critical access (CA) violations, and establish access management governance for sustaining a compliant environment. These can be very costly and burden internal resources if you need to redesign, test, and re-implement a compliant solution after going live.

Security and access management governance should be one of the cornerstones to implementing a compliant solution. The security model must be designed in a way that it supports the business, but without introducing risk to the organization. In addition, the compliance and security teams cannot be the roadblock to moving forward with critical implementation milestones or even go-live. This means compliance must be agile and quick to assess risk and/or provide compliant solutions, which can be a challenging task

during critical phases such as testing. In this paper we will focus on aligning with the overall implementation and aligning efforts during the critical phases irrespective of methodology.

Tools for Success

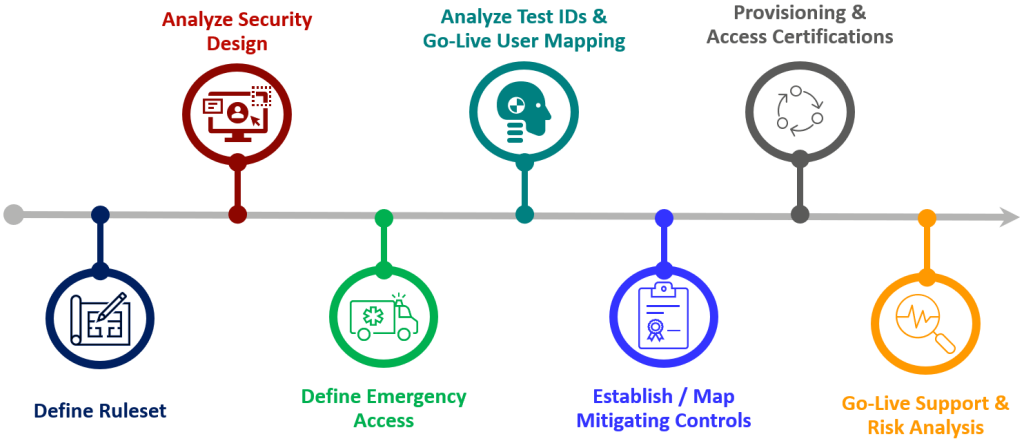
Before diving in, it is important to enable our compliance team to be successful. The right tools and technologies must be in place for our teams to provide their value. It is not uncommon to couple the ERP implementation with the rollout of a new access management tool or compliance platform. Regardless, to be successful, the compliance organization needs the capability to systematically assess access risk and implement access management controls. The most mature organizations leverage the full capabilities of their tools to streamline and automate their access management efforts across a variety of applications and assess the true cross-application risk universe.

At Fastpath, our quick-to-implement, easy-to-use, cloud-based platform provides the necessary capabilities to manage and monitor access risk across your landscape. Founded in 2004, Fastpath now has more than 1,000 customers across the globe and in a variety of industries. The Fastpath Assure® compliance platform comes equipped with out-of-the-box connectors to many of the popular ERP, HCM, and CRM applications, including SAP, NetSuite, Microsoft Dynamics, Oracle, Workday, Salesforce, and more. Leveraging these connectors, organizations can support their compliance efforts to assess SoD and CA access risk and manage access within a single or cross-application environment.

Fastpath is traditionally reviewed or discussed once a system is already established or, even worse, after an audit concern such as a significant deficiency or material weakness exists. However, augmenting the compliance team with Fastpath Assure can streamline efforts and instill confidence at the time of go-live.

Managing Risk with Fastpath

Below is a breakdown of how our Fastpath customers leverage Assure during an ERP implementation or upgrade. The access management governance principles highlighted below are applicable irrespective of the supporting technology.



Define SoD and CA Ruleset

Establishing the baseline SoD and CA ruleset is the foundation of a compliant security model. Regardless of whether you are starting from scratch or updating an existing framework, the requirements of the new system must be evaluated for inclusion in the ruleset. This baseline is then revisited throughout the implementation and beyond. Triggers for changes could come from design review, testing, cutover, during hypercare, or while sustaining the solution beyond go-live.

The SoD and CA ruleset should be comprehensive of the organization's risk universe. As processes begin to span across multiple applications and interconnected systems, so should the ruleset design. If vendors are maintained in a master data system and payments are generated out of another, the risk for fraudulent activities now spans across multiple applications. As such, the SoD ruleset should consist of cross-system risks to accurately monitor and manage access risk. This is the foundation of managing access risk. It is imperative that the appropriate stakeholders are involved to provide an overview of the process, establish risk criticality, confirm customizations, define risk ownership, and more.

Security and access management governance should be one of the cornerstones to implementing a compliant solution.

The Fastpath Assure solution comes with out-of-the box connectors enabling you to connect and monitor access risk across a variety of ERP platforms and business applications. In addition, Fastpath provides out-of-the box rulesets that can be tailored to meet each organization's respective needs. With the Segregation of Duties module, you can mass import or design SoD cross-system or CA rules within the Fastpath UI itself. The scalability Fastpath Assure enables allows organizations to develop and maintain a ruleset with audit logging throughout the implementation.

Analyze Security Design

Once the SoD and CA ruleset has been established, access risk can be evaluated. Leveraging a compliance platform, such as Fastpath Assure, enables you to streamline access risk analysis during critical phases of the project. This should be an iterative process starting in the design phase to ensure security entitlements are being designed in a compliant manner. This is a pinnacle of a best-in-class security architecture, enabling SoD conflict-free environments or only introducing risk when multiple components are assigned to a single-user account and/or can be mitigated.

Fastpath's customers can leverage standard functionality to systematically perform detective and preventative access controls throughout the implementation. This is a critical capability when facing tight timelines and responding to change from a variety of trigger events. This is also where we begin to see the value in the "design-in" approach because the next steps

we take in our journey are performed with a compliant security model. If testing is performed with SoD conflict-free security, we know the system will work with a collection of access. If we identify risk in subsequent phases, we can assign access with more granularity in efforts to remediate the risk or follow the principle of least privileged. When access cannot be remediated, we look to mitigate the risk with compensating controls or responsive controls such as emergency access.

Define Emergency Access

Sometimes, access is required irrespective of sensitivity or risk. Plus, every organization is different. Whether it is driven by the organization's industry, regulatory obligations, or organizational differentiators like intellectual property and/or recipe information, the scope of emergency access varies. Emergency access, also known as Firefighter or Privileged Access Management (PAM), is another instrumental tool to controlling and monitoring access across the landscape. Depending on your ERP, you may even leverage SYSADMIN, Administrator, or other scenarios to perform activities with temporary escalated access.

During the COVID-19 pandemic, we observed workforce reduction, children learning virtually, colleagues out sick or taking care of loved ones, and other circumstances that contributed to increasing the number of use cases for backup duties across the business and IT. Defining the appropriate use cases for emergency access is only one piece to the puzzle. It is critical to establish what access should be restricted, who should approve the assignments and audit logs, and frequency of reviews, to name a few more.

We see higher long-term costs for organizations that must go back and redesign or retrofit their solution with compliant controls.

Knowing the answer to these questions early in the design process help implementation teams design day-to-day access and supporting processes. Augmenting these processes with Fastpath Assure's Emergency Access module can streamline the execution and audit activities of this process. Utilizing workflow-enabled approval processes and activity monitoring, the tool stores the necessary details for future audits and review.

Analyze Test IDs & User Mapping

Security professionals may say that designing security without SoD conflicts is somewhat easy. Managing a collection of access to support business and IT processes is another story. Not every organization operates the same. In most cases, organizations do not even have standardized processes from one location to another. These conditions can translate to a collection of access with SoD conflicts potentially requiring remediation or mitigation.

From an implementation standpoint, identifying this access risk prior to critical phases in the project can prevent additional clean-up efforts down the road. While there could be multiple testing phases in a single implementation, ensuring the application works as

expected with a compliant security model should be on the checklist. This can be done by enforcing compliance "checkpoints" prior to testing cycles. Re-performing user mapping or even redesigning the security could be required if security access is not assessed prior to testing or go-live. If risk is identified after go-live, the risk could potentially require immediate remediation or mitigation leading to an additional allocation of resources.

Partnering with Fastpath to perform the risk analysis on security roles/entitlements and users before and after testing phases can streamline these critical "checkpoints". Fastpath Assure modules Security Designer and Segregation of Duties offer features to perform integrated or ad-hoc risk analysis before introducing the changes into testing or production environments. The simulation or "what-if" analysis acts as an additional preventative control to maintain the compliant security architecture beyond the go-live.

Establish/Map Mitigating Controls

It is not uncommon to have processes supported by workflows, mandatory review/approvals, configurations, and more, that mitigates risk. These mitigations or mitigating controls, are often leveraged in the instance access risk is present and emergency access or access remediation is not an option. It is important to find an appropriate balance when defining acceptable mitigating controls as organizations can quickly find themselves allocating resources to performing a strenuous amount of control validation activities on top of their day-to-day duties. This can also lead to the manual control becoming more of a "rubber stamp" activity diminishing the effectiveness of the control.

This is another domain where the pre-work provides value and reduces potential costs in the future. When risks are identified post go-live, a mitigating or compensating control would have to be developed and tested/validated, as well a potential lookback to prove fraudulent activities were not performed within the exposure period. When aligning with the ERP implementation, we can leverage the Segregation of Duties module to systematically assess user mapping and respond accordingly prior to go-live. Once it has been determined that the identified risk cannot be remediated, a mitigating control can be identified, entered in the Fastpath Assure control library, applied, and reported on systematically within Fastpath Assure. Auto-mitigation and finite rule-based mitigations can be configured to further streamline future review efforts or quick reporting on mitigated risk.

Provisioning and Access Certifications

Leading up to this point, all the focus has been on designing a compliant security model, testing with compliant test IDs and user assignments, as well as defining processes to mitigate access risk that could not be avoided at the time of go-live. It is imperative prior to going live critical processes such as compliant user provisioning/de-provisioning and periodic access certifications are in place. These processes enable the compliance team to implement preventative and detective access controls and sustain the compliant design implemented.

To be effective, key stakeholders (e.g., requestors, approvers, etc.) should be trained on the processes and technologies prior to go-live.

The most basic breakdown of a user provisioning process is one where some form of a trigger event or request is reviewed, approved, and actioned accordingly. This is often performed with a ticketing system, emails, manually actioning the request, etc. With the Fastpath Identity Manger module, user provisioning is streamlined through a customizable workflow-driven process integrating SoD and CA violation checks as a preventative control. Once approved, Fastpath Assure automates the provisioning/de-provisioning to the connected systems within the landscape eliminating manual activities and potential human error. Additionally, features such as ticket mapping and approval logging are leveraged to facilitate future reviews and audits.

If vendors are maintained in a master data system and payments are generated out of another, the risk for fraudulent activities now spans across multiple applications.

Periodic access certifications are another key component in the sustaining phase. This detective control traditionally consists of supervisors and/or security entitlement owners reviewing access assignments for the user/ security entitlements to which they are assigned. Access can then be approved or rejected from the respective users. The Access Certification module in Fastpath Assure automates this traditionally manual process by collecting the in-scope access assignments, routing assignments to the configured reviewer(s), and automating the de-provisioning processes by generating an access request if an assignment is rejected. The dashboarding reports provide visibility and tracking of this process. The frequency of the reviews traditionally depends on criteria such as user population size, geographical disbursement, turnover rate, external audit guidance, and more.

For compliance professionals, having the capability to perform these processes across a variety of applications is imperative. Thinking back to the first section, Define SoD and CA Ruleset, a critical component is to capture the access risk across the interconnected systems within the landscape. The ability to assess access risk across multiple applications is a critical input into the provisioning process. This is where Fastpath Assure's ability to connect to a wide array of applications out-of-the-box combined with features such as role templates and approval groups to further streamline complex processes with integrated control points. In addition, the dashboarding features provide insights to reviewers and management on outstanding requests and overall status of certification processes with additional drilldown capabilities.

It is worth noting that user provisioning is a critical component throughout an ERP implementation, managing the access for project stakeholders across the landscape. Access to the sandbox, development, quality/test, and future production environments change at

an incredible rate during an implementation. Managing these access requirements should be controlled to manage risk. As an example, designing and provisioning security under specified naming conventions for quick validations that project security roles are not present in production at the time of go-live. While this will not be the focus, it is important to monitor/manage this aspect with project risk management.

Go-Live Support & Risk Analysis

All the work has been leading up to this moment: Go-live. Following the "design-in" approach we included the compliance teams as key stakeholders and can approach this date with confidence. As a recap, we know the security architecture is SoD conflict-free, the application and processes have been validated with compliant security assignments, emergency access processes have been defined, the mitigating controls are established and mapped, go-live user mapping has been assessed, and sustaining processes have been established. These activities when paired with other implementation success factors (e.g., organizational change management, thorough testing, successful data loads, etc.) set the organization up for a successful go-live.

Managing access in preparation of go-live and during the hypercare period can be quite stressful. This is only magnified when security and compliance is an afterthought during the implementation. When compliance is not included, we often see the initial risk analysis uncover large volumes of SoD and CA conflicts. Addressing this risk is no easy task. Typically, security must be redesigned, testing is reperformed, user mapping is updated, etc. In addition, compensating controls or additional manual tasks must be performed to prove fraudulent activities did not take place while the exposure was present. Even worse, external audit may designate significant risk exposure leading to deficiencies or material weakness. These are a few examples of those higher long-term costs when compliance does not get to play a role in the implementation.

It does not matter if it is a greenfield or brownfield implementation, you leverage waterfall or agile methodology, or compliance was included from day one, there will be go-live issues to address. From a go-live support perspective, a variety of issues typically arise related to data, configuration, security, training, and others. When additional access is required, Assure's Identity Manager provisioning processes with integrated SoD and CA conflict analysis are leveraged, break/fix issues are addressed with the Emergency Access module when privileged access is required, new customizations and/or requirements follow the "design-in" approach being considered for ruleset, and so on. It is all about working the process. There is no scramble to clean up excessive access or manual error-prone processes to login and provision/deprovision access. These are the benefits realized when integrating the compliance team in the implementation or upgrade.

Summary

Once the dust settles, one journey comes to an end and another begins. It is important that organizations protect their investment and manage risk through compliant access management processes and principles. Baselining access risk exposure and measuring success through KPIs and metrics across all the compliance processes should be performed from the onset and then revisited on an appropriate frequency for the organization. The overall number of conflicts by criticality and unique risk exposure by user/role are two examples of KPIs to measure from an exposure standpoint. Also, performing periodic reviews of the SoD and CA ruleset, emergency access usage, and number of mitigated risks are a few others which may indicate process or access changes are warranted.

About Fastpath

Founded in 2004, Fastpath has deep expertise in audit, security, and compliance, with multiple Certified Internal Auditors on the team. Fastpath has global partnerships with several audit firms and a client base which spans across multiple industries within both publicly traded and privately-held companies. Fastpath Assure® is a cloud-based audit platform that can track, review, approve and mitigate access risks across multiple systems from a single dashboard.

Visit our website for additional resources like this eBook, on-demand webinars, and more.

For a live demonstration that targets your specific requirements, please contact us.