



Measuring the **ROI** of internal control automation





ROI

Calculating a return on investment (ROI) for internal control automation isn't easy. Most executives know that the potential damage from a cybersecurity threat or material misstatement can be severe: disruption of operations, reputational damage, loss of customers, and regulatory penalties.

But control failure costs are potential costs, and internal control automation programs are actual costs, making automation initiatives a hard sell. So, how can you identify and quantify the ROI of internal control automation in an environment where buyers are inundated with buzzwords and new technologies that sometimes succeed but often fail?

What are internal controls, and what is control automation?

Internal controls are policies, procedures, and IT mechanisms designed to create safeguards against damage or loss. More specifically, internal controls are activities that:

- Increase operational efficiency
- Protect the accuracy of your data
- Ensure appropriate access and use of your IT systems
- Maintain compliance with regulations, and
- Defend against fraud and data theft

Manual controls rely on human intervention. Automated controls, on the other hand, are control activities that are performed automatically through a system or software. Strong internal controls are essential to governance and critical enablers for growth and operational efficiency. Reliance on manual controls has limitations because of its dependence on error-prone human intervention.



How to calculate ROI

Buyers and executives are looking for assurances that their investment in new technology will produce a return. And that **return on investment** is typically defined as *“a financial ratio used to calculate the benefit an investor will receive in relation to their investment cost. It is most commonly measured as net income divided by the original capital cost of the investment. The higher the ratio, the greater the benefit earned.”*

Automated access governance solutions can produce ROI in the following ways:

- Time saved in application access provisioning
- Efficiencies gained through SOD automation
- Improved access certifications
- Privileged access management
- Operational efficiency gained through faster employee onboarding
- Reducing inherent risk in roles assigned to users in **ERP systems**

Before using SafePaaS, a multinational corporation with thousands of employees manually performed identity and access governance responsibilities utilizing a combination of on-premises and homegrown tools that required significant upkeep and time because their solutions were not integrated. The customer’s lack of integration and manual efforts exposed them to a high risk of security breaches, non-compliance penalties, audit fines, and potential reputational damage. After their investment in SafePaaS, the customer gained efficiencies by streamlining several internal identity and access governance processes, such as application and employee access provisioning, access certification, and segregation of duties (SOD) tasks. This eliminated 20 hours of work annually for 10,000 managers and compliance staff, resulting in a cost savings of \$10,000,000.

– **10,000 managers worldwide to certify the access of their staff**

– **\$50 per hour at 20 hours per year for 10,000 managers = \$10,000,000**

“According to Gartner, a company with 10,000 employees can realize an ROI of approximately 300 percent and save \$3.5 million over three years simply by switching to automated provisioning.”

The problem with ROI

While this ratio can help you lay the groundwork for calculating ROI where you have no previous investment, it lacks the context to explain how you can achieve ROI in an environment where you have already invested in technology with minimal return.

Most internal control automation solutions tend to focus on specific aspects of internal controls, like **ITGCs** or **ICFRs**. These solutions may relieve your pain points, but their ability to deliver ROI is limited. The ability to truly deliver ROI is only as good as a solution's integration with your existing technology.

In the case of **identity and access management** and **ITSM solutions**, the ROI gained is minimal due to their lack of integration capabilities. Because most of these solutions cannot integrate with your existing technology, **they create new pain points diminishing their ROI.**



The highest ROI is generated in three ways:

1 Alignment between strategy and risk across the enterprise:

Organizations must govern resources by executing strategy. What gets in the way of execution is a risk. Risk can happen anywhere, and leadership needs a governance platform that looks at the complete enterprise and everything in it to manage the business effectively.

2 Integration of execution activities:

SafePaaS bring it all together in a unique platform which ensures that these activities are creative, collaborative, and integrated as opposed to operations occurring in silos. This drives your processes to align with governance objectives.

3 Controls embedded in processes:

By embedding controls into your operations, you are the first to know if there is a control failure. This allows you to PREVENT control failure before you lose business to competitors or incur a hefty penalty in the market. Therefore the ROI is higher.

Where your company is losing productivity during audit

The following are the top challenges internal control automation solutions create when they cannot integrate with your existing technology.

Segregation of Duties – SoD presents significant challenges for almost every company, regardless of size. Every year organizations overlook the cost and risk that not remediating and controlling their segregation of duties conflicts has on their bottom line.

Verifying SoD violations in a fine-grained audit involves digging through dozens of screens in your ERP for hundreds of users to investigate potentially conflicting job responsibilities. Evaluating thousands of complex security and configuration settings through manual research on error-prone spreadsheets is inefficient and substantially decreases the organization's productivity. This is because most solutions on the market only report on this risk; they don't manage the risk through remediation.

During an audit cycle, auditors task companies with reviewing and correcting these fine-grained privilege conflicts. Organizations usually turn to consultants to run a one-time **SoD assessment** report of their ERP security configurations. From this one-time assessment report, a team of staff (compliance officers, process owners, IT Service team, and Internal audit) will spend 3-5 hours quarterly reviewing each SoD policy violation in a spreadsheet. To get an idea of how much time is spent quarterly on verifying SoD policy violations, let's look at an **example**:



Company with 10,000 employees

1,000 managers and staff to review the SoD assessment report

5 hours/per quarter spent on SoD violation review @ \$50/hr for each reviewer

5,000 hours at \$50/hr = \$250,000 per quarter or \$1 million annually

Add **on top** of the \$1 million spent reviewing the assessment report from the example above; **you still have the work and cost associated with external audit findings. Each audit finding requires remediation efforts from the same staff in the example, resulting in twice the effort of review for a total of up to \$2 million annually just for SoD violation analysis.**

Many organizations opt to outsource analysis and remediation due to the amount of work involved in reviewing policy violations and remediation. However, the cost of hiring consultants is generally 3 to 5 times more than internal staff rates. The SafePaaS platform can reduce the burden and cost of SoD analysis and remediation by 80% - 90% delivering an ROI of up to 500% in the first year.

SafePaaS can generate up to 500% ROI by:

- Streamlining the SoD management process through the automation of policy violation analysis. The system automatically removes false positives and other flagged access to the system while preventing these violations from appearing in future SoD policy violation reports.
 - up to 50% reduction of flagged violations in future analysis cycles - saving time and effort
- Violation surveys are automatically sent to control owners through an automated workflow for remediation. Managers can review violations, correct the role design, and submit the redesigned role for automatic remediation.
- SafePaaS' automated workflows reduce up to 80% of the effort spent on violation analysis and remediation. This is an ROI of up to 500% in the first year. ROI continues to grow as other risks are treated, recorded, and excluded from future violation reports.



Inadequate user provisioning

A significant challenge with IAM is the lack of visibility into **fine-grained privileges**. IAM solutions only allow you to request access at a role level and don't provide visibility into what that underlying access entails. Without understanding the underlying access, you may be unknowingly creating segregation of duties conflicts.

Time to provision and deprovision access, consistency of provisioning, a central source of truth, and management of a single identity are all benefits that provide security with the added benefits of knowing who has access to what and when and, more importantly, why.

ROI of user provisioning - Through policy-based user access provisioning, SafePaaS automatically provisions proper access and de-provisions inappropriate access. In addition, SafePaaS simplifies granting added access safely through access and approval workflows.

Lack of privileged access management (PAM)

Most IAM solutions allow you to request **privileged access** and create workflows for approval. However, that is where the support for PAM ends. These tools do not monitor what users do in your system, track when privileged access was taken away, or record what the user did in the system while they had privileged access.

ROI of PAM - SafePaaS FireFighter provides on-demand privileged access management with built-in monitoring and reporting capabilities. FireFighter privileged access enables organizations to temporarily elevate emergency access permissions while simultaneously controlling the risk that elevated permissions can introduce.

No user activity monitoring in your ERP

Many organizations struggle with **lookback analysis** during their external audits when former employees retain access after departure. During your audit, you will be required to provide evidence that the departed employee didn't log in to your system and tamper with data or perform other malicious actions. IAM solutions don't offer insight into user actions once in your application.

ROI of user activity monitoring - Save time and stress during your audit digging through archived data. SafePaaS allows you to take snapshots of your enterprise system to reconstruct a past year's audit and investigate a past event. This is a unique feature of SafePaaS. SafePaaS allows you to set the snapshot intervals to create a separate audit history. With SafePaaS, your data is kept in a separate vault, enabling you to go back to any historical point. If you discover a problem, you can see what the data looked like each year and see who had access.

Insufficient user access certification

IAM solutions that are not integrated with your other applications cannot support access certification because they cannot provide the entire picture of user access across the IT landscape. Integrated identity governance is required to prevent security threats and streamline operations to mitigate inherent application risks.

ROI of automatic access certification – The manual process of reviewing user access privileges requires weeks per application to complete. SafePaaS enables you to complete an access certification automatically, eliminating hundreds of hours needed to perform access certification.

Outdated ITSM catalog

Managing user access requests from ITSM systems also creates a headwind on ROI because ITSM systems rely primarily on a catalog of abstract roles that need to be manually mapped to the ERP system and then determined whether that user should have access. While ITSMs enrich your basic roles with privileges and attributes, without a governance solution, your ITSM is not governed by company policies and is vulnerable to error and risk.

ROI of customized role design – Many organizations face challenges when granting roles and access to applications. To ensure that the user's access fits their role and your information security policies, you need a policy-based governance solution that only permits a safe combination of privileges and attributes.



ROI Assessment

Managing controls manually is impossible due to the cost and risk associated with human error. When done correctly, control automation can enhance compliance, lower costs, reduce cyber vulnerability, and allow staff to work on value-generating projects.

Organizations should consider what is lacking in their existing control automation solutions and integrate their existing solutions to create a system that spans across on-premise and cloud applications. At that point, the organization will reap the full benefits and generate ROI by boosting user experience, reducing cyber risk, streamlining processes, and placing processes around policies from the top down so that you're always strategically aligned and generating the highest potential for ROI.

If you want to learn more about how your company can benefit from an enterprise-level governance platform that connects, automates, and integrates your business talk to us. We can drive the ROI specifically for you and your business.

Still not convinced? Here are a few more examples of how we helped our customers maximize their ROI:

- **20% reduction** in internal controls testing from 136,000 hrs to 108,800 @ \$50/hr = \$1.36M per year
- **20% reduction** in external controls testing (SOD) expense from 12,000 to 9,600 @ \$165/hr = 0.4M per year (*immediate value)
- **Reduction in cost** of retesting failed controls = \$0.4M per year (*may occur in yr 2-3)
- **Reduction in external audit fees** = \$0.4M per year (*may occur in yr 2-3)

Ready to maximize your ROI?

For a more detailed discussion to see how SafePaaS can help you maximize your ROI, please contact:

Emma Kelly
Senior Marketing Manager
emma.kelly@safepaas.com

3300, Dallas Parkway, Suite 200,
Plano, Texas, 75093 USA