

# Analyzing the Total Cost of Ownership for Manual Access Management in U.S. Enterprises

Security breaches and compliance failures can lead to significant financial and reputational damage. In 2023, the average cost of a data breach was [USD \\$4.45 million](#) worldwide, which is a 15% increase over the last three years. Companies incur nearly [\\$15 million](#) in expenses due to non-compliance repercussions, which is 2.71 times more than the cost of maintaining compliance through robust compliance programs.

And again - the damage can also be reputational. According to a report by Forbes Insights, [46% of organizations](#) experienced damage to their reputation following a data breach, and 19% faced reputational and brand harm due to security breaches involving third parties.

All of this points toward the importance of efficient access management in enterprises. It's key to be aware of the Total Cost of Ownership (TCO) associated with manual requests for access workflows and processes, as well as manual access certification or attestation processes in enterprises across the United States. This analysis seeks to shed light on the financial and operational impacts of these manual processes and how the shift toward automated solutions can offer substantial benefits.

## The Necessity of Access Management in Modern Enterprises

Access management is essential for security, compliance, and operational efficiency. It involves controlling who has access to which resources within an organization, a task that has become increasingly complex with the proliferation of digital assets. In the U.S., stringent regulatory environments such as HIPAA (for healthcare) and SOX (for finance) necessitate meticulous access management practices to avoid legal repercussions and safeguard sensitive information.

## Components of Manual Access Management Processes

- **Manual Request for Access Workflows:** Traditionally, these workflows involve a series of steps where employees request access to resources, and managers or IT administrators approve or deny these requests based on necessity and policy. This process is often paper-based or managed through spreadsheets and emails, making it cumbersome and error-prone.

- **Manual Access Certification or Attestation:** This involves periodic reviews where managers or IT administrators verify the appropriateness of access rights granted to users. It is critical for compliance and security but can be time-consuming and fraught with the potential for oversight.

## Calculating the Total Cost of Ownership

- **Direct Costs:** The labor involved in managing manual access requests and certifications is significant, requiring dedicated IT staff time and managerial oversight. Administrative overhead, including managing paperwork and communications, adds to the cost.
- **Indirect Costs:** Manual processes are inherently less secure and more prone to error, increasing the risk of security breaches. Compliance risks also loom large, with potential fines and penalties for failures. Moreover, the opportunity costs in terms of lost productivity and the diversion of resources from strategic initiatives are considerable.

## Industry-Wide Analysis

A comparative analysis across industries reveals that sectors with stringent regulatory requirements, such as healthcare and finance, bear a higher TCO for manual access management due to the complexities and risks involved. The analysis also considers the impact of industry-specific regulations on TCO.

So what exactly does that mean? Consider healthcare breaches, which carry significant repercussions for both providers and patients. In 2023, the average expense of a healthcare breach soared to almost [\\$11 million](#), marking an increase of over 50% since 2020, as reported by the Ponemon Institute and IBM Security. Remember that the average cost of a data breach is \$4.45 million - so again, certain industries have more at stake than others.

## Manual Vs. Automated Processes

Manual access management processes are plagued by inefficiencies, high error rates, and scalability issues. Significant operational challenges and security incidents can arise from these outdated practices, and professionals emphasize the urgent need for more efficient solutions.

Automation and Identity Access Management (IAM) solutions present a promising avenue for reducing the TCO associated with access management. Automated systems can streamline workflows, reduce errors, ensure consistent policy enforcement, and

offer scalable solutions that grow with the enterprise. Automated processes offer long-term savings and operational benefits.

## Implementing Automated Access Management Solutions

For enterprises seeking to transition from manual to automated access management processes, several steps are critical. Key considerations include assessing current processes to identify inefficiencies; selecting the right tools and solutions that align with organizational needs; prioritizing scalability and compliance; and promoting training and awareness to make sure that new practices are successfully adopted and adhered to.

## Conclusion

The TCO analysis of manual requests for access workflows and processes, alongside manual access certification or attestation processes, reveals significant financial and operational burdens on enterprises. The move towards automated solutions promises cost savings and enhanced security and compliance postures. More and more enterprises are reevaluating access management processes in light of TCO findings. This strategic move becomes imperative, and the shift from manual to automated access management is a critical step toward securing and optimizing enterprise operations.