OpenText Identity Governance for your business

As business owners take control of their digital services, they inherit ultimate responsibility for their success. While productivity and consumer engagement are the primary ambitions of these services, they need to be secured in order to minimize their risk to the organization.

Benefits

- Gain powerful insights into measuring the risk associated with granting and maintaining permissions to users and processes
- Increase governance consistency across your environment
- Work seamlessly across your hybrid environment
- Get unmatched policy enforcement, modular dashboards, and hundreds of adjustable correlation rules

Whether for internal or consumer-facing processes, business owners are now leading the transition to digital operations and providing the vision to drive it to completion. This is a significant shift from past practices, where IT owned the budget, the implementation, and the operational support of those digital services. However, as these business owners drive digital transformation to increase efficiency and establish new business models, they also inherit shared responsibility for new challenges and security.

Business owners pulled into compliance complexity

One of the toughest realities for organizations is that, while they have been driving the evolution of their business models and supporting digital transformation practices, they have also been pulled deeper into securing it.

Government mandates mature

The public's increasing dependence on digital services, along with the brisk rate of breaches, has been a driving force for governments to respond with more robust protections. At first, they were vague suggestions, but they have become less discretionary and much more concrete.

As these regulations have transformed from best practices into mandates, agencies have become keenly aware of their importance. And, because they

emphasize privacy and segregation of duties, these mandates involve a library of details that organizations need to understand as they determine how to apply them in their business.

Competing priorities

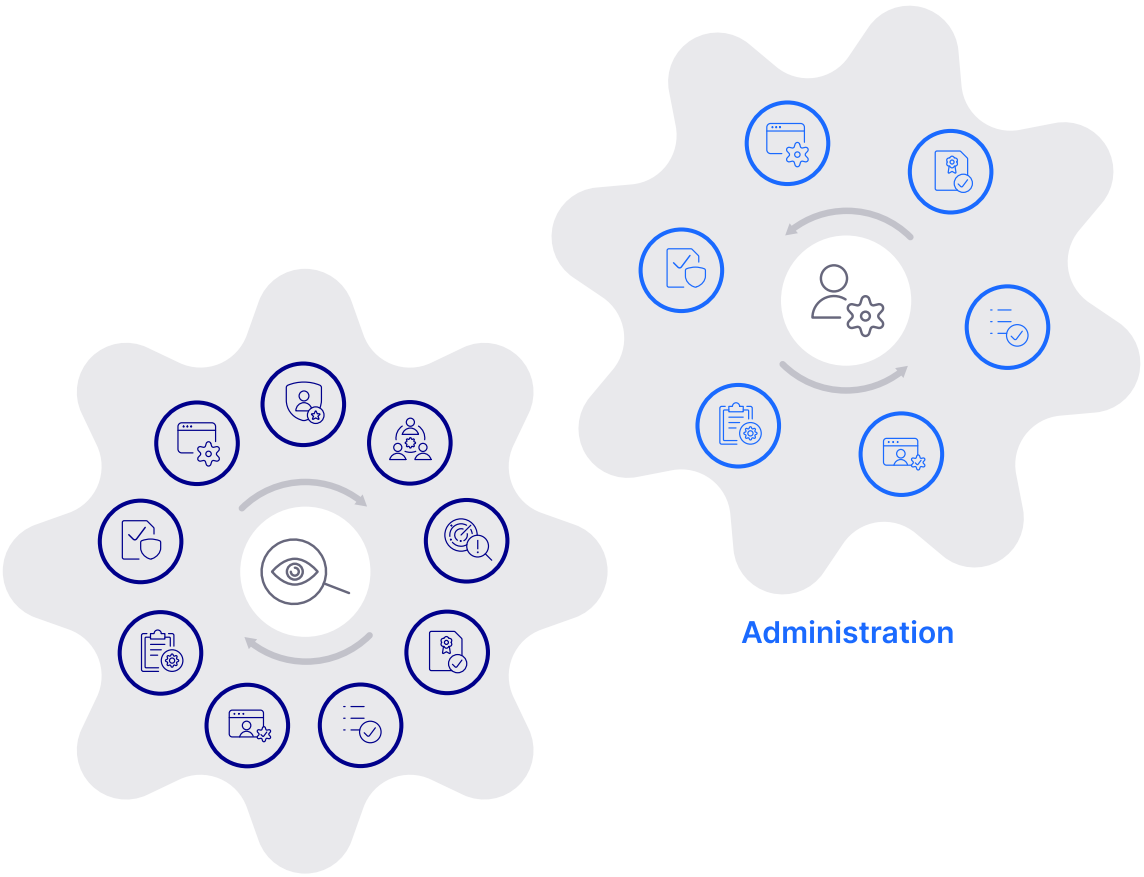
One of the realities that an organization must consider is that their information handlers aren't security or compliance officers; compliance enforcement is only one of their many responsibilities. These professionals have pressing requests relative to their primary responsibility, while also ensuring that they properly govern access to the sensitive information they manage.

Confidence to digitally engage

While business owners have leveraged SaaS-based services to advance their ventures, they have also inherited the responsibility of governing who has entitlements to them, especially if neither IT nor the security teams are overseeing their security.

The rising cost of risk

Ponemon Institute's annual Cost of a Data Breach Report documented that in 2024 the average cost of a data breach in the US was $4.88M.[1] Verizon's comprehensive annual Data Breach Investigations Report (DBIR)[2] provides a concrete taxonomy of different types of digital security attacks, as well as an analysis of their tracked frequency. We know from this study that organizations have not made significant headway in driving down the frequency of breaches. These two reports can serve as foundational components for business justification for funding robust risk management.



1 Ponemon Institute, *Cost of a Data Breach Report,* 2025
2 Verizon, *2025 Data Breach Investigations Report*

Resources

Check out our YouTube channel ›

Keeping your mandate commitments

Beyond managing your digital risk, you need a well-balanced entitlements strategy that keeps your organization efficient and effective, while staying compliant with the segregation of duty (SoD) mandates. In addition to SoD, you need to enforce a least-privilege model that maximizes privacy without crippling services delivered to the consumer. As organizations compete to engage their consumers more effectively, this can be a difficult balance to strike.

OpenText Identity Governance for the business

OpenText™ Identity Governance provides information and services owners with the tools they need to successfully govern entitlements to their information:

- It enables the business to make more informed and consistent decisions about which access requests should be granted and which ones should be denied.
- It collects entitlement data across your infrastructure (cloud, off-cloud, and hybrid).
- It presents relevant and insightful information to approvers in a simple format that can be quickly assessed.
- It automates request workflows, focusing attention on people, processes, and resources that pose the most risk to the organization.
- It enables approvers to make better access decisions through unique business insight available from its analytics engine.

With a comprehensive set of OpenText identity governance and administration services, OpenText Identity Governance helps you achieve the right level of access to meet your compliance needs. And through its real-time recognition and responses to out-of-policy permissions, it also drives down your risk.