SafePaaS™

CORESTREAM

Learn

Why GRC and Access Governance are the Digital Enterprise's Perfect Partners

By Paul Cadwallader and Adil Khan

Table of Contents

Governance, risk, and compliance (GRC) programs are designed to protect the company, its stakeholders, and its reputation by ensuring compliance with laws and regulations, mitigating risks, promoting ethical behavior, and enhancing operational efficiency. Companies can adopt a solid governance framework for sustainable and responsible growth by adopting GRC programs.

However, governance frameworks (SOX, EURO-SOX, BASEL II) primarily address business processes and risk management, with little recognition of the underlying IT and IT risk management processes. These areas are often approached separately, creating silos in the organization.

Implementing and executing governance frameworks in silos reduces the quality of mitigation because risks are managed in isolation. The first step to address this issue is integrating GRC and access governance processes. Integration of GRC and access governance facilitates the identification of corresponding identity data, roles, and information flows between the various risk management processes.

Defining GRC and Access Governance

GRC is much broader than most realize. GRC is about how the various segments converge to help an organization act efficiently and ethically when coupled with access governance.

Governance: the system of control that ensures an organization performs well and delivers its strategy. It provides the framework of accountability and oversight to ensure that activity is well managed.

Risk management: risk management identifies and manages potential problems (and opportunities) to make achieving objectives more likely. The key to effective risk management is to be proactive by looking forward to identify potential issues.

Compliance: adherence to the regulations, policies, and contractual obligations.

Access Governance: Access Governance, also known as Identity Governance or Identity Governance and Administration (IGA), refers to policies, processes, and tools used to control unnecessary or excessive user permissions and enforce appropriate access to sensitive data and digital assets. Ensuring users only have access to data necessary for their role within your organization (a concept also known as Zero-trust), which mitigates the risk of cyberattacks that exploit excess privileges and helps organizations meet increasingly strict compliance standards for privacy and data protection, such as GDPR, ISO 27001, and the NIST Cybersecurity Framework.

Access Governance is not the same as Access Management. Access Management is about identity management or Active Directory, where you put someone in the network when they start at your organization, give them some privileges, and they have access. Access Governance defines security processes and policies for the enterprise's data management.

Challenges that businesses are facing today?

Accessing information is important for your organization as you move to digital business platforms, whether an ERP, CRM, on-prem, or in the cloud. Access governance has become a key opportunity and challenge for organizations.

Integration and interoperability

Organizations' most significant challenge in meeting GRC and access governance objectives is integrating systems and point solutions where identity and access data are stored. For example, you may use Okta or Azure to manage your user identities, an ITSM like ServiceNow to grant access, and your HCM for timesheets and expenses. The difficulty in connecting these stores of user identity data requires an identity hub that can define the identity and privileges for access across all environments, detailing how users request access, how user access gets fulfilled, and ultimately approved and provisioned.

"Granting too little access can reduce productivity and create bottlenecks. Give too much access, and you risk fraud and cybersecurity threats." - Adil Khan, CEO of SafePaaS.

Entitlement complexity

In a typical digital platform, you deal with multiple security models and privilege hierarchies. For example, seeded roles are used in most business systems because they offer out-of-the-box functionality. However, these "seeded roles" are complex and have inherent risks. Seeded roles require fine-grain visibility into the role structure to identify risk. For example, a Payables Manager may contain privileges that enable that user to create AND pay suppliers, causing a segregation of duties violation and an increased risk of fraud. However, this conflict of privileges may be acceptable from a security perspective because that user cannot change the bank accounts. Each role must be examined to ensure security.

Data privacy

Data is a top concern for consumers, and your organization's ability to protect that data is critical. Your ability to secure sensitive systems, processes, and data hinges on your ability to lock down user access.

The data protection problem is solved by implementing data access governance. You need to ensure that the right people have access to the right data and that your ITGC controls are effective.

As vendors introduce new features and functions or you introduce new roles into your organization, there's a risk that someone gets excessive access to data.

ITGCs are the core of your controls framework, and when your ITGC controls aren't automated, the business is exposed to risks. We recommend monitoring the access and ensuring that the access complies with the policies for access. However, it's a challenge with such huge volumes of data and many data sources. For example, today, some organizations have data on requisitions where people can submit their own requisitions, and there's data on employee health and supplier information. All these data points are protected, but the policies don't enable governance by themselves, meaning a lot of time is wasted on writing good policies that aren't embedded in the system - leading to a lack of data governance.

Siloed organization

Because of siloed business functions, adopting cloud and SaaS-based solutions is easy - as simple as clicking a button. The ability to govern resources and data in your organization is a real challenge and headache for those wanting to provide access to the company's data. The silo-based approach of acquiring systems and managing access is unsustainable. Organizations need a holistic, collaborative framework that will be the key to integrating access governance with GRC and management.

Operational dimensions

Access management and governance requirements move faster than your organization's overall governance and policies. This creates a disconnect between overall governance and access governance or "who can do what, and where." Operational governance becomes disconnected from access governance due to the need to respond to your current organizational drivers. Joining governance efforts is a big challenge for managing risk and demonstrating compliance with customers, regulators, and auditors, all driving those demands.

Drivers

Digital transformation

Many organizations are transforming their business and operating models to respond to changing market demand. Operations are now executed online, creating an opportunity to re-engineer your organization's framework, structure, and processes about how the organization functions—getting access and governance integrated to understand the risks and threats to your organization.

Zero-trust

Adopting approaches like zero-trust means having a handle on access governance to manage access risk. Executives have far more focus on access risk than ever before, and they're starting to understand the interconnectedness of risks. If you manage access risk effectively, you get successful outcomes that mitigate reputational damage and regulatory pain from customers, auditors, and shareholders.

Move to hybrid environments

Work is now flexible and fluid, particularly as extended enterprises continue, so you rely on organizations outside your business to deliver part of your services or products. Because outside third parties access your data and systems, that hybrid environment of the extended enterprise is another big factor in the need to join GRC and access governance.

Regulations

The regulatory environment is increasing in complexity and scope, no matter your industry or business size. Whether this is for assurance and attestation, increased focus on supply chain security, or data privacy, your organization needs to look at its overall control framework and approach to risk, including managing access governance. With this shift in perspective, the focus is on improvement in risk and compliance maturity. These drivers will also help propel the adoption of GRC and access governance.

Inefficiencies

The fragmentation of the access governance process creates several inefficiencies. Bottlenecks can bog you down and create audit fatigue. Sometimes that also accelerates into an audit finding, a significant deficiency, or even a material weakness, which is a death sentence for a company because you have to spend unlimited amounts of time and resources to resolve the issues and keep them from reoccurring. Trying to do that in spreadsheets and standard reports is a fool's errand because most IT people haven't taken in-depth audit and risk management classes or studied or worked in that field. This can feel like you're being pinged for issues you don't fully understand. Joining GRC and access governance helps your team return to the jobs they were hired to perform.

Use cases to unify GRC and Identity Access Governance

Zero trust

Zero trust is a key pillar to a successful cyber program. And so, locking users out and giving them only what they need to perform their role is a reason organizations are starting to respond to access risk.

Extended enterprise

Organizations are beginning to realize the need to lock down third-party access to your systems where they perform services on your behalf, either from outsourcing a business function or because their business model needs distributors or franchisees. You need to trust third parties and manage their access to your resources. Again, a policy-based access governance approach to governing that access to monitor ongoing risk for third parties, comply with the relevant laws and regulations on your behalf and manage their access.

Joint ventures

Often joint ventures (JVs) have many external parties involved in the operation of your organization. And in certain circumstances, those organizations, for example, oil and gas companies, come together into JVs to explore and extract oil and gas. Each brings relevant commercial and competitive data flows. Access governance can be used proactively to firewall off secondees from each company in the JV from seeing information related to another. It's critical in managing risk and regulatory requirements from an antitrust perspective around data flow, particularly commercially sensitive information.

Segregation of duties

In key processes like the record to report or procure to pay, you highlight your risks and put in the controls to mitigate those risks through management certification, attestation, and independent controls testing.

For example, you may have a control restricting users that enter and post journals or create suppliers and pay suppliers. These may be the high-level policies in your GRC module. Unifying that with your access governance policies means you have true governance across the enterprise. It's one thing to design a control; it's another to verify its operational effectiveness. And to do that requires information from the GRC platform and generating the SoD policies mentioned above. Unified GRC and access governance catches that and prevents conflicting privileges from being provisioned into your system. When the two systems are unified, you can break down silos, optimize your business, and become a proactive GRC organization. You can integrate your controls framework in your GRC software with access controls and policies that actively monitor user activities in your digital platform where you execute business.

Top benefits of unified GRC and Access Governance

Driving standardization, automation, and efficiency

Driving efficiency is the first aspect around access governance and how that feeds into the wider risk landscape, and conformance reporting that will flow up an organization. Access governance is part of managing the overall flow of information about your risks as an organization and how you manage those risks within your governance framework.

Holistic management of risk

Organizations are becoming very fluid, with people continually changing roles to meet the needs of businesses. Organizations have more flexible models and traditional ways of working. The ability to have agility in policy and structure, rather than rules in access governance, is key to managing risk-agility through the technological capability enabled by integrating GRC and access governance.

Efficiency

Governance is a fragmented process in most mature organizations because it's siloed. Because access is scattered throughout the organization, it tends to be reactive and siloed, which means that some controls are over-tested, and some are missed completely. That's how you end up with audit fatigue and findings. Organizations need to move toward integrating their GRC activities and access governance into a single platform to eliminate barriers and become more efficient and proactive.

Common vocabulary

Once an organization has a common vocabulary regarding risk, it becomes easier to talk about access controls and access governance. Managing risk and user access becomes easier for all process stakeholders once they have a shared set of terms and actions for carrying out processes and controls.

Active Governance

You want a system that actively monitors policies and processes so you are not burdened by looking over your shoulder. You need to embed controls within the processes enabling you to block user conflict by performing activities that can cause a compliance issue or audit finding. Active governance is the guardrail of active controls. Active controls sit in the background monitoring and prevent the risks from occurring because these controls are preventive, not authoritarian.

Access Governance is essential for GRC because it helps organizations maintain security, meet compliance requirements, manage risks, allocate data and resources efficiently, and establish accountability. It is a critical component of a comprehensive GRC strategy, ensuring access to essential resources and data is controlled and monitored effectively.

Contact Us

From a solution perspective, know what you need, understand those needs, and work with your teams to identify critical requirements. Lean on vendors because they deal with requirements' challenges every day. Vendors can help guide you in terms of how they help address specific needs.

CoreStream is a provider of market-leading, next-generation GRC (Governance, Risk, and Compliance) / EHS / ESG solutions. The platform provides a solution that is both user-friendly and user-focused. The CoreStream Platform can be tailored through simple and rapid configuration to meet every client's need and deliver an integrated GRC experience to help organizations achieve their true business potential.

The platform works seamlessly in tandem with clients' processes and procedures, its flexibility and adaptability providing them with a solution that encourages proactive decision-making, collaborative working on compliance and assurance, and supports governance through accountability. Crucially, the platform also offers both time and cost savings as you embed it in your processes.

SafePaaS is the policy-based access governance platform that automatically detects and prevents audit findings and security incidents across the entire enterprise in one single platform.

Built from the ground up, our organic, agile cloud platform allows organizations to adopt and extend identity security, access governance and process governance solutions efficiently and effectively when required.

SafePaaS supports any enterprise application, any cloud infrastructure, any IAM or ITSM system for complete governance. Policies sit at the center of our platform architecture delivering immediate value without the complexity of role-based IGA solutions.

CORESTREAM

https://www.safepaas.com
https://www.corestream.co.uk/

SafePaaS™