ConductorOne

What DevSecOps Teams Need to Know about Identity Governance and Administration (IGA)

Identity governance and administration (IGA) is a policy-based approach to identity management and access control. Adopting an IGA strategy gives you powerful tools for controlling access within software systems. This article explores what IGA is, why it matters to DevSecOps teams, and the changes it enables within your workflows. You'll learn how IGA principles can be used to support provisioning, compliance, and security requirements for your DevSecOps processes.

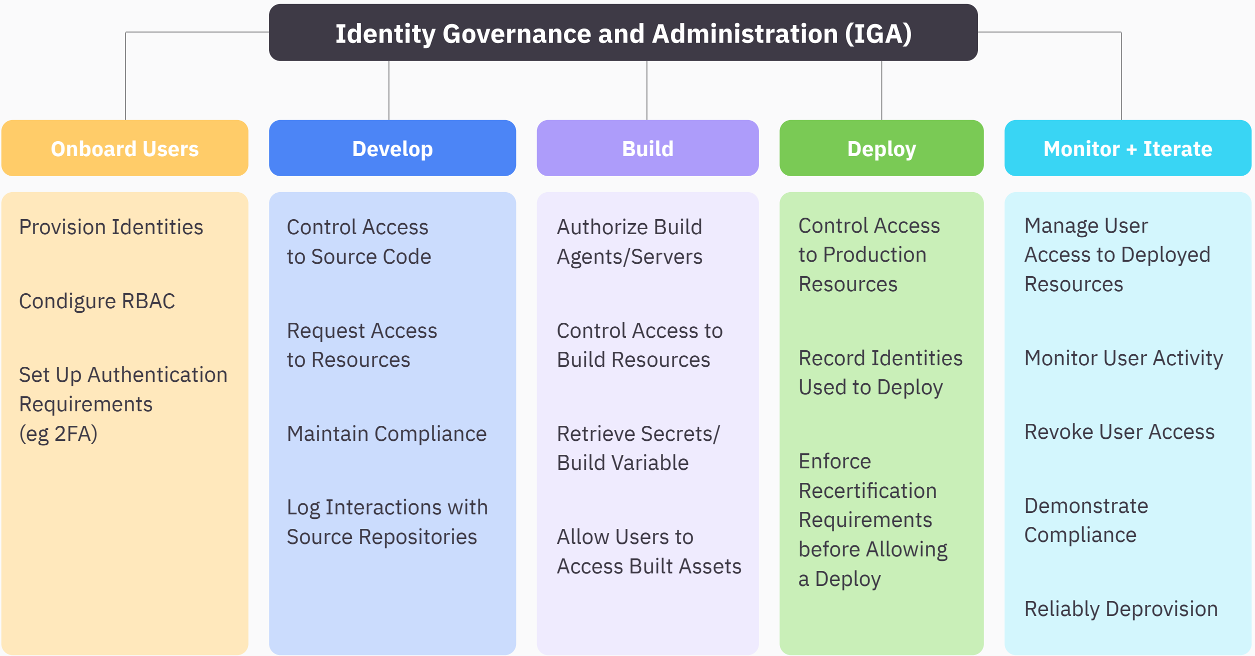
What Is Identity Governance and Administration (IGA)?

IGA refers to processes and tools that security and IT teams use to manage user identities and access controls across their environment. IGA solutions offer centralized identity management, with features such as automated user provisioning, self-service access requests, segregation of duties (SoD) enforcement, role-based access control (RBAC), user access reviews, incident detection, and reporting for compliance.

IGA supports a "shift left" approach to identity management. IGA providers can usually integrate into your existing DevSecOps processes for automated identity operations alongside development workflows. While commonly associated with larger teams, IGA is equally beneficial for smaller organizations that want to maximize automation and security for their operations.

How Does IGA Impact DevSecOps Workflows?

IGA presents a pragmatic approach to access control, where all access-related functions are controlled by a single system. IGA functionality is supplemented by robust automation, compliance, and risk management features that collectively strengthen security and reduce operational overheads. But how does this map to existing DevSecOps workflows?



Identity Governance and Administration (IGA)

Onboard Users

- Provision Identities
- Condigure RBAC
- Set Up Authentication Requirements (eg 2FA)

Develop

- Control Access to Source Code
- Request Access to Resources
- Maintain Compliance
- Log Interactions with Source Repositories

Build

- Authorize Build Agents/Servers
- Control Access to Build Resources
- Retrieve Secrets/ Build Variable
- Allow Users to Access Built Assets

Deploy

- Control Access to Production Resources
- Record Identities Used to Deploy
- Enforce Recertification Requirements before Allowing a Deploy

Monitor + Iterate

- Manage User Access to Deployed Resources
- Monitor User Activity
- Revoke User Access
- Demonstrate Compliance
- Reliably Deprovision

Improve Access Provisioning and Deprovisioning

Many organizations still rely on manual processes to onboard users, grant them access to resources, and make changes as requirements evolve. This is time-consuming and error prone; it creates friction that prevents new users from becoming productive until an admin has fully provisioned their accounts. Similarly, when users leave the organization, there's a risk their accounts will remain active until an administrator remembers to take action.

IGA allows you to integrate user provisioning and deprovisioning operations into your DevSecOps workflows. You can use the automated tools and processes you're already using for software development, such as IaC and CI/CD pipelines, to configure your identities and then roll them out to your IGA platform.

This produces a simple, standard, and scalable mechanism for onboarding users and applications. Instead of admins needing to manually work through long-winded manual processes, they can add the user to the IaC config file, declare which resources should be accessible, and then wait for the pipeline to run to completion. The IGA solution will then create the identity and set up applicable access controls, such as allowing the user to access relevant Git repositories, build servers, and ops applications.

IGA also facilitates the timely revocation of access from unused or compromised identities. Users can be deprovisioned either based on a manual action—such as removing the account from an IaC config file—or as a result of an automated policy, such as account inactivity or suspected abuse. This ensures that unused identities don't linger within your organization, which helps to reduce your attack surface and prevent ex-employees from continuing to access resources.

Enforce Role-Based Access Control (RBAC)

Controlling access and authorization is hard, particularly for distributed teams where apps, infrastructure, devices, and user identities are frequently changing. Users should only be able to access the resources they actually need for their responsibilities. This requires a robust role- and permission-led approach to ensure the correct constraints are applied throughout the DevSecOps process. IGA solutions support this requirement through the inclusion of RBAC capabilities.

Managing RBAC at the IGA platform level lets you set up roles and permissions once, then use your policies to control user access to all your apps and infrastructure assets. It reduces repetition and lowers the risk of oversight.

As with identity provisioning, IGA also allows you to automate role assignments and revocations within your existing DevSecOps processes. You could implement pipelines that automatically assign the correct roles and permissions to new identities based on the team they're joining and the projects they're involved with. This further reduces the strain on administrators by fully integrating identity operations with your organization's workflow.

IGA also helps support self-service access to resources. If a team member needs to access another app, they can request it through the IGA platform. Typically, the platform is configured to send an alert to an administrator; once approved, the user's existing permissions are automatically expanded to include the new app.

Promoting automated self-service access also further reduces the workload for admins. It helps prevent important access provisioning steps from being missed and can shorten the time that users must wait while access requests are reviewed. This tightens the DevSecOps feedback loop, improving efficiency without sacrificing the powerful granularity of RBAC.

Achieve Continuous Compliance

IGA isn't just about automating identity operations within your DevSecOps workflow. It also solves the challenge of how to continually preserve compliance while supporting the identity requirements of fast-paced development items.

By centrally managing identity provisioning and access control, IGA guarantees that changes to identities will align with your compliance requirements. All alterations are ultimately applied by the IGA solution, meaning there's a single destination to inspect during compliance audits and incident investigations. This contrasts with traditional ad hoc identity management processes, where information and actions are disseminated across multiple independent systems without any central logging.

Certification, audit, and reporting capabilities are similarly essential tools for organizations that must maintain compliance with specific standards. IGA platforms usually include these facilities, allowing you to capture events, analyze user access patterns, and highlight any potential noncompliance risks.

IGA's self-service capabilities can be beneficial to compliance as well. Less identity information is shared throughout your organization when users can submit access requests through an IGA platform. IGA also supports painless certification and recertification processes, for example, by requiring users to reauthenticate before they can submit an access request.

IGA is therefore an effective way to achieve continuous compliance within existing DevSecOps workflows. Using automation to integrate identity management into DevSecOps processes avoids the compliance challenges of having administrators manually interact with accounts.

Orchestrate Security Incident Responses

Security incidents are best viewed as unavoidable to encourage preparedness and prevent complacency. IGA is a powerful tool you can add to your arsenal to spot and respond to access-related security incidents, such as an access control breach or attempted use of expired credentials.

IGA platforms provide an overarching view of the identity-related events that are occurring within your organization. This degree of visibility enables rapid detection of new incidents by allowing you to track who is accessing different resources. If an unexpected access attempt is logged, then you can use the platform to begin further investigations.

Captured audit logs, attestations, and change records provide the information necessary to support incident response efforts. These can help you pinpoint where and how the incident began, as well as how it progressed and the actions that have occurred since. The data can also be useful if you need to demonstrate to regulators, customers, or clients that you retained governance of identities and user data during a suspected incident.

Integrating IGA with DevSecOps routines allows incident management workflows to be combined with your existing development processes. This can speed up response times by affording a unified reaction to incidents. The ability to quickly determine what happened, take steps to mitigate the impact, and apply any required process changes—all from one integrated platform—permits efficient and confident incident resolution. Compare that with a non-governed approach to identity management, where figuring out which account caused a breach—then taking steps to contain it—can require hours of manual trawling by administrators, if the relevant data is even available.

Conclusion

This article explored how you can use identity governance and administration (IGA) to improve operational efficiency and enhance security protections as you manage user identities. IGA goes beyond familiar concepts such as IAM to support organizations in administering, automating, and auditing identities. It provides a stable platform for defining and enforcing access control policies.

To decide whether you need IGA, determine the pressure facing your teams as they perform identity management tasks. If account provisioning, deprovisioning, access requests, and user access reviews and reporting are creating bottlenecks in your processes, it could be time to introduce a modern IGA solution like ConductorOne. ConductorOne is designed to help organizations streamline identity governance, allowing DevSecOps teams to minimize time spent on admin while ensuring access controls are consistently applied. Book a demo or take a product tour to learn more.