Meeting Regulatory, Framework, and Standards Obligations with Okta Identity Governance

The Identity management and access control imperative

Today's organizations require a holistic, integrated approach to Identity management that not only allows governance to play a crucial and connected role with access management, but also helps to strengthen security posture, mitigate modern risks, improve efficiency, and even enhance overall productivity.

For each user, Identity management enables effective onboarding and continues throughout their lifetime at the company — which may include lateral moves, promotions, and other role changes — until they move on and their access is revoked.

Identity management also extends to the adoption of new applications and the introduction of third parties like contractors and partners. Many factors complicate Identity management: hybrid IT environments, the increased role of software-as-a-service (SaaS) applications, and remote working arrangements — to list only a few.

For many teams, these processes were once (or still are) manual, which is risky, costly, and burdensome to IT, HR, and department leads.

The risks are especially pronounced for organizations that must comply with regulatory requirements or adhere to standards, where an inability to meet these compliance expectations can grow to have board-level impacts on organizations.

—

Because of its essential role in securely connecting users to the technology and resources they need, Identity requirements are frequently included within a wide range of regulations, frameworks, and standards.

What are some of the most common Identity controls organizations need to implement?

How can organizations use Identity Governance and Administration (IGA) to meet compliance obligations?

What are the benefits of doing so beyond satisfying regulatory and certification body needs?

In this guide, we'll explore these questions and share additional best practices and tidbits to help today's organizations excel in the digital age.

IGA is a policy-based approach to Identity management and access control that combines:

- **Identity governance:** Processes and policies that cover the separation of duties, role management, logging, access reviews, analytics, and reporting
- **Identity administration:** Account and credential administration, user and device provisioning and deprovisioning, and entitlement management

By merging these two components, IGA systems provide additional functionality beyond traditional **Identity and Access Management (IAM)** tools.

An IGA system's ability to automate workflows for provisioning and deprovisioning users strengthens Identity security and creates a detailed historical record of activities — helping organizations meet compliance requirements and satisfy the information needs of audits.

At the same time, this high degree of automation improves process efficiency and enables increased workforce productivity.

Identity's role in compliance

Within the broader domain of governance, risk management, and compliance (GRC), IGA is vital for protecting customer information, securing sensitive financial data, and protecting resources from being tampered with or inappropriately shared beyond organizational boundaries.

The more efficiently and effectively an organization can execute on IGA, the better positioned it is to:

- **Manage regulatory risk** by complying with even the strictest Identity controls
- **Access new customers** by meeting third-party risk thresholds
- **Build and maintain a strong, least privilege security posture** and inform risk-based cybersecurity programs
- **Achieve market differentiation** with standards and certifications that raise the bar on competitors
- **Increase overall productivity** by simplifying lifecycle management, which helps new employees to be productive on day one and throughout their time with the organization as their roles change and grow

Representative regulations, frameworks, and standards

Here are three widely adopted regulations, frameworks, and standards, picked from the worlds of accounting, security, and privacy.

Sarbanes-Oxley

Following a number of financial scandals, the Sarbanes-Oxley Act (also called Sarbox or SOX) was enacted into law in 2002. The aim of SOX was to improve investor confidence by making corporate practices more transparent. Among others, requirements include measures for:

- Policy enforcement
- Risk assessment
- Fraud reduction
- Compliance auditing

Because most of the data making up corporate financial statements is created by information technology systems, **carefully controlling access to these systems via IAM and related controls is vital to Sarbanes-Oxley compliance.**

SOC 2

SOC 2 (Service Organization Control 2) is a cybersecurity compliance framework designed to ensure that third-party service providers securely store and process client data.

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 reports on organizational controls based upon the five trust services principles of:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

With threat actors increasingly targeting Identity for initial access and to execute intrusions, and with 97% of organizations planning to have a Zero Trust initiative in place by early 2024, **robust Identity-related controls are an essential component of a strong security posture.**

PCI

The Payment Card Industry Data Security Standard (PCI DSS, or simply PCI) is a proprietary information security standard for companies that manage major credit cards.

Full compliance means companies encrypt payment card data in transmission, submit to penetration testing, and more. PCI doesn't mandate specific technologies but explains industry best practices. For instance, there are certain PCI requirements about limiting — to the absolute minimum — the number of employees who can access payment card data.

Proper Identity management practices help to maintain the privacy of payment card data by carefully restricting who can access this information and when.

Common Identity controls

While the specifics of each regulation, framework, and standard vary, the Identity-related requirements overlap significantly and tend to address three main areas.

Organizations — especially large enterprises — often have to meet many controls simultaneously, and these controls frequently have different requirements for the same subject.

For example, one framework may demand that passwords be changed every 90 days, while another may call for changes every 60 days.

In such a scenario, **a recommended best practice is to use a common control library: a single control that incorporates the highest bar from each regulation, framework, and standard that applies.**

Taking this "high bar" approach allows the organization to meet the strictest requirements as effectively and efficiently as possible.

Identity security

As adversaries focus greater attention on attacking Identity systems — including leveraging stolen credentials — organizations must implement strong security measures that help to prevent malicious access to applications, data, and other resources.

Consequently, many regulations, frameworks, and standards specify controls pertaining to:

- Password configuration: strength (e.g., length and complexity), frequency of change, etc.
- System security: multi-factor authentication (MFA), federated access through secure systems

Password configuration and system security are closely related. For example, if a federated identity is managed via an IAM system that requires all employees to use MFA, then this higher degree of security may supplant requirements to change passwords every 90 days.

Access controls

In general, access controls ensure that the right people have the right access to the right resources when they need it — ideally with the least amount of friction.

To create a strong security posture and to manage privacy risks, such controls also typically incorporate the principle of least privilege (or logical access), which limits each user's access — and their granular rights such as read, write, execute — to only those applications, resources, and other assets needed to do their job.

In practice, implementing access controls requires careful consideration of:

- "Birthright" and "non-birthright" access: Distinguishing between resources (e.g., applications, data sets, etc.) that a user can access on day one (as a "joiner") versus those that require additional approvals
- Access requests and approvals: Establishing processes by which users can request additional access, and by which approvers (e.g., manager, IT administrator) can review and approve (or deny) requests
- Access reviews: Controls that verify (periodically or triggered by an event) that only legitimate users have access to resources
- Access certification: Essentially, re-approvals to ensure each user has appropriate levels of access

In addition to implementing these controls, organizations may also be required to produce reports (e.g., to achieve certification or at the request of auditors) that capture who has what level of access to what resources today and who had what level of access to what resources in the past. Consequently, maintaining access controls is necessary but insufficient: detailed logs must also be kept.

A general assessment of an individual's access and certification of access are often grouped together, but in reality, they address different aspects of Identity governance.

For example, an access assessment verifies that a particular user's general role hasn't changed and can, therefore, still have access. An access certification goes further and assesses whether or not that employee's level of access is still appropriate (e.g., perhaps they are no longer on a particular project).

Separation of duties

Separation of duties (also known as segregation of duties) is a key administrative control intended to minimize the occurrence of:

- Errors
- Deliberate acts of fraud, sabotage, theft, policy violations, misuse of information, etc.
- Other security incidents, including data breaches

The basic mechanism by which separation of duties controls work is by preventing overlaid IT access that would allow compromising activities; in other words, such controls ensure that no one person acting alone can complete a particular sensitive task. These access capabilities that would allow compromising activities are called "toxic combinations."

In practice, such controls may be needed throughout the organization. For example, an individual user should not be able to:

- Request *and* grant access to a resource (e.g., application, data, etc.)
- Raise *and* approve a purchase order
- Perpetrate *and* conceal errors or fraud
- Write code *and* promote it into production

Implementing and maintaining separation of duties requires IT teams to scalably account for organizational changes (e.g., promotions, demotions, transfers, etc.) and new technology adoption, combined with conflict role definition and a rule set that accounts for toxic combinations.

When a user logs in to a computer system, what they're permitted to do depends on what access controls are in place. For example:

- **Role-based access control (RBAC)** allows administrators to grant access based on role characteristics like department, location, seniority, and work duties.
- **Attribute-based access control (ABAC)** enables more nuanced controls by allowing administrators to set permissions based on the user, resource attributes, environment, and other factors.

Whether or not a particular regulation, framework, or standard specifies the use of RBAC or ABAC, **an effective access control solution greatly simplifies implementing and maintaining Identity-related controls.**

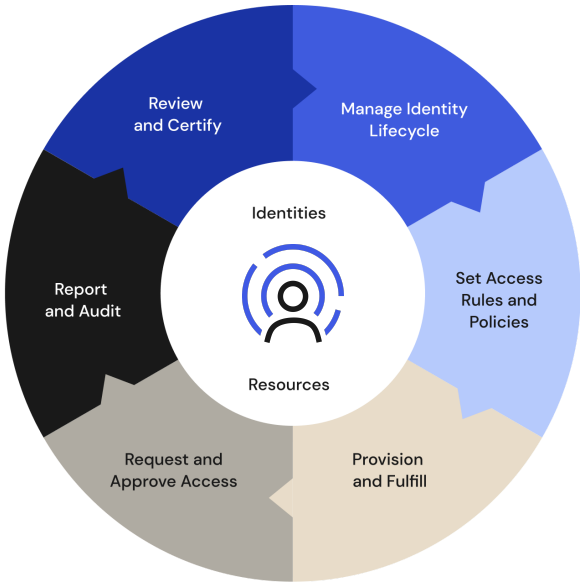
Learn more about RBAC and ABAC

Meeting obligations with Okta Identity Governance

Okta Identity Governance is part of a SaaS-delivered, unified IAM and governance solution that adds three new **access governance** capabilities to the Okta Workforce Identity Cloud.

- **Okta Access Requests** uses self-service capabilities, tightly integrated with popular collaboration tools, to simplify and automate access requests and approvals.
- **Okta Access Certification** makes it simple to create and manage recurring and automated access review campaigns and to configure recertification campaigns with appropriate resource owners.
- **Enhanced Governance Reports** provide comprehensive out-of-the-box reporting capabilities to help meet audit and compliance requirements.

Combined with lifecycle automation capabilities powered by Okta Lifecycle Management and customization and extensibility offered by Okta Workflows, these capabilities empower organizations to fulfill compliance obligations in a less burdensome fashion while unlocking many other benefits.



Here are three ways to improve and more efficiently achieve compliance outcomes within your organization:

- Deliver a great user experience by integrating with popular tools and providing context to reviewers; this approach reduces the burden on individual stakeholders by meeting them where they are.
- Leverage automated provisioning to lower the risk of errors and to lessen the amount of manual work.

- Delegate tasks to optimally share the workload; for example, IT can help configure access request processes but doesn't necessarily need to be involved in approving actual access requests.

Example: Birthright access

Okta Lifecycle Management's group-based provisioning feature enables organizations to automatically provision applications and groups based on user attributes.

This approach reduces the demands on IT teams and helps new employees get up and running on day one — without the long periods of waiting that characterize many onboarding experiences.

Because provisioning is based on user attributes (e.g., defined in HR solutions like Workday) and corresponding groups, access is appropriately tailored to each individual's role.

In addition to the added efficiency and lowered risk of error that comes with automation, the **tight integration of Okta's unified solution makes it easy to enforce strong security standards.**

For example, when an application like Salesforce (SFDC) is integrated with Workforce Identity Cloud through SAML, SFDC relies upon Okta as the federated user store to authenticate incoming SFDC users.

When a user's federated Identity is secured by MFA, this added security extends to SFDC. Plus, this arrangement can automatically meet or exceed the strong password requirements that are part of many regulations, frameworks, and standards. For instance, an organization might be obligated to force users to change their SFDC passwords every 90 days, but this need is met by demonstrating that the federated Identity is protected by MFA.

Example: Access requests and approvals

From a compliance perspective, it's critical to have a solid process governing who has access to resources and to be able to show how access was provided to each user.

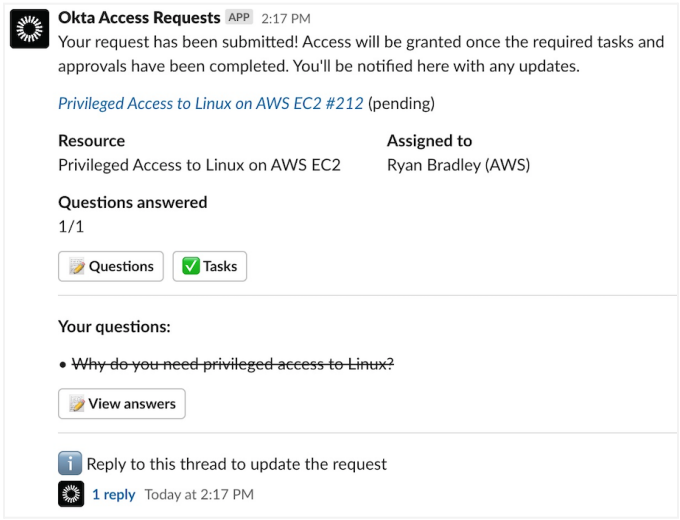
Okta Access Requests makes life easier for all stakeholders by meeting requesters and approvers where they are and by helping administrators quickly deploy a powerful access request process.

- Requesters can use the collaboration tool they're most familiar with — like Slack or Microsoft Teams — to create a new access request to the resource they need.
- Approvers are quickly notified and can choose to approve or deny the request from within those same tools or in the web UI.
- Administrators have access to a powerful — but simple to use — workflow builder, allowing them to quickly build new request flows containing one or more approval steps, with individual conditions to determine when the approval is required, what actions should be executed, and even what conditions would trigger an action.

Because of Access Requests' flexible and customizable workflow builder, GRC and IT teams can partner to build scalable request workflows that tap the correct approvers — from people managers to resource owners — to instill compliant access request processes.

[See a demonstration of access requests and approvals]

By meeting users where they are — in this case, in Slack — Okta Access Requests lowers friction for everyone



The benefits of an access request and approval process that's easy for everyone to use extend well beyond compliance.

For example, **fast approvals mean users aren't waiting to access** necessary applications and resources, so productivity improves.

Plus, **with no reason to bypass the approvals process, the risk of "shadow IT" and other dangerous circumventions is reduced**.

Example: Access certification

To fully operationalize least privilege principles, organizations must ensure users don't accumulate resource accesses that are no longer required.

Traditionally, access certification campaigns run on a periodic schedule. But many organizations are also implementing event-based certifications triggered by reorgs, acquisitions, security incidents, major project milestones, etc.

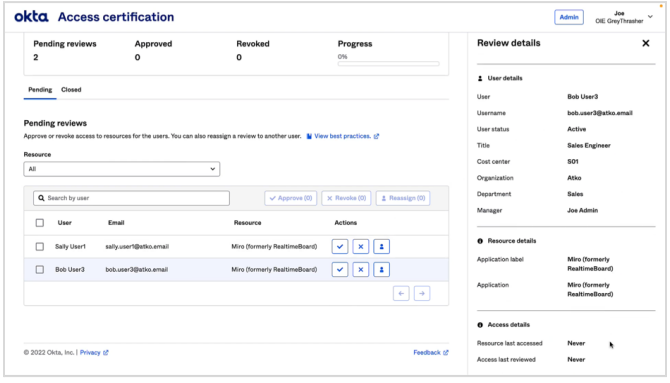
In addition to meeting compliance requirements, running campaigns more frequently helps manage risk. It can also reduce operating expenses by eliminating unnecessary license fees. But to secure stakeholder buy-in and avoid the practice of "rubber stamping" (i.e., just re-approving access without any consideration), such campaigns need to be easy to configure and execute.

As with Access Requests, Okta's Access Certification combines power and ease of use to minimize time and number of clicks without compromising on governance.

- Campaigns are configured by following a simple five-step process.
- An emphasis on flexibility and customization makes it easy to configure campaigns for the right reviewer or multiple levels of reviewers.
- Integration with Okta's IAM capabilities provides reviewers with a complete picture of the user, the resource, and the user's relationship with the resource, enabling quick — but informed — decisions.
- Access Certifications and Workflows can trigger re-assignment of users and revoke access.

[See a demonstration of an access certification campaign]

Integration with Okta Workforce Identity Cloud means reviewers benefit from additional context, like when a user last accessed an application



Because of the traditional difficulty of performing access assessments and certifications, many organizations perform them only because they have to (practically every compliance framework requires them) and only as frequently as required.

But in reality, the value of such campaigns extends well beyond compliance obligations. They serve as an important and effective backstop against costly — and potentially hazardous — access accumulation.

Example: Separation of duties

Meeting separation of duties requirements involves configuring and managing complex rules to reveal "toxic combinations" of roles.

It's this type of Identity process customization that's addressed by Okta Workflows, which makes it possible to automate Identity processes at scale — without writing code.

Once administrators have identified toxic combinations, Workflows' if-this-then-that logic, pre-built connector library, and ability to connect to any publicly available API enables organizations to implement proactive controls (i.e., when access is being assigned). Leveraging those same toxic combinations, Okta Access Certifications can be used for reactive controls (i.e., as part of periodic violation audits and reports).

In practice, separation of duties controls:

- Leverage standard Okta data objects, events, and tables
- Can use Workflows to assess any Identity object that can represent a set of IT accesses
- And often employ fine-grained accesses tied to application functions

Example: Reports

Most regulations, frameworks, and standards include reporting requirements — but beyond showing auditors and certification bodies particular Identity controls are in place, reports can also help organizations make informed business decisions and investigate security incidents.

Okta Identity Governance offers a variety of out-of-the-box reports, including:

- Application Usage Report: Data about who has signed in to an individual app integration or every app integration during a specified time period
- Past Campaign Summary Report: High-level configurations and status of access certification campaigns, allowing review of the types of resources covered in each campaign and its completion percentage
- Past Campaign Details Report: In-depth information about any or all certification campaigns, with the ability to filter to include a set of specific resources or users, remediation status, or certification status, among other data points
- Past Access Requests Report: Who has requested access to resources, including whether access was granted and by whom
- Entitlements and Access Reports: Monitor the activity and security of your organization, manage user access to resources, track resource usage to reduce licensing costs, and help meet audit and compliance requirements

Okta's reporting is query-able to meet specific information needs efficiently and conveniently, allowing GRC and IT teams to customize reporting for whatever resource or user subset any given compliance audit requires.

Conclusion

Meeting compliance needs and adhering to a broad set of regulations is critical for organizations to continue to manage regulatory risk.

While IGA is an essential element of many regulations, frameworks, and standards, the benefits of meeting compliance thresholds extend well beyond managing regulatory risk.

By effectively implementing Identity security, access controls, and separation of duties capabilities, organizations will improve their overall security posture, access new customers, differentiate themselves from competitors, and increase the productivity of their workforce — all while relieving the IT department and other stakeholders of many administrative tasks.

But becoming compliant and benefiting from the additional value IGA can deliver is predicated on finding an IGA solution that can deliver on those governance promises without the costly implementations and burdensome upkeep that complex tooling often imposes.

A new way forward

Okta Identity Governance changes the equation by making Identity governance and administration accessible and affordable, with:

- **Quick time to value:** Turn months of implementation into days for immediate returns without prolonged disruption.
- **Straightforward scalability:** With a cloud-native solution and over 7,000 pre-built integrations, you'll be able to automate complex Identity processes at scale.
- **Out-of-the-box integration with the Okta Workforce Identity Cloud:** Leverage a unified IAM and governance solution to unlock new efficiencies that enhance security and productivity.