



Take the Sting Out of Compliance With Modern Identity Governance

Sam Katzen

Group Manager, Product Marketing, Okta

Agenda

-
- 01 Identity's role in compliance

 - 02 Best practices and approaches from the field

 - 03 Okta Identity Governance: modern IGA

 - 04 Showcasing Okta Identity Governance

 - 05 The IGA benefits beyond compliance

 - 06 Q&A



Identity's role in compliance



What is GRC?



“A well-coordinated and integrated collection of all the capabilities necessary to support principled performance at every level of the organization.”

*Open Compliance and Ethics Group definition



Identity management

ensures the right people have
access to the right resources for the
right amount of time



Sarbanes–Oxley

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

Carefully controlling access to information systems via IAM and related controls is vital to Sarbanes–Oxley compliance.



PCI (Payment Card Industry Data Security Standard)

PCI is a proprietary information security standard for companies that manage major credit cards.

PCI explains industry best practices like 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.



SOC (Service Organization Control)

SOC helps illustrate the strength and security of an organization's data protection.

SOC 2 reports on organizational controls based upon the five trust services principles of:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

Robust Identity-related controls are an essential component of a strong security posture.



Common Identity controls



Identity security

- Password configuration
- System security



Access controls

- “Birthright” and “non-birthright” access
- Access requests and approvals
- Access reviews and certification



Separation of duties

- Prevent “toxic combinations” that allow a single individual to complete compromising activities



Best practices and approaches



Thoughts from the front lines

Evelyn Ngai
Director, Business Technology, GRC



Bill Cox
Director, Security Compliance



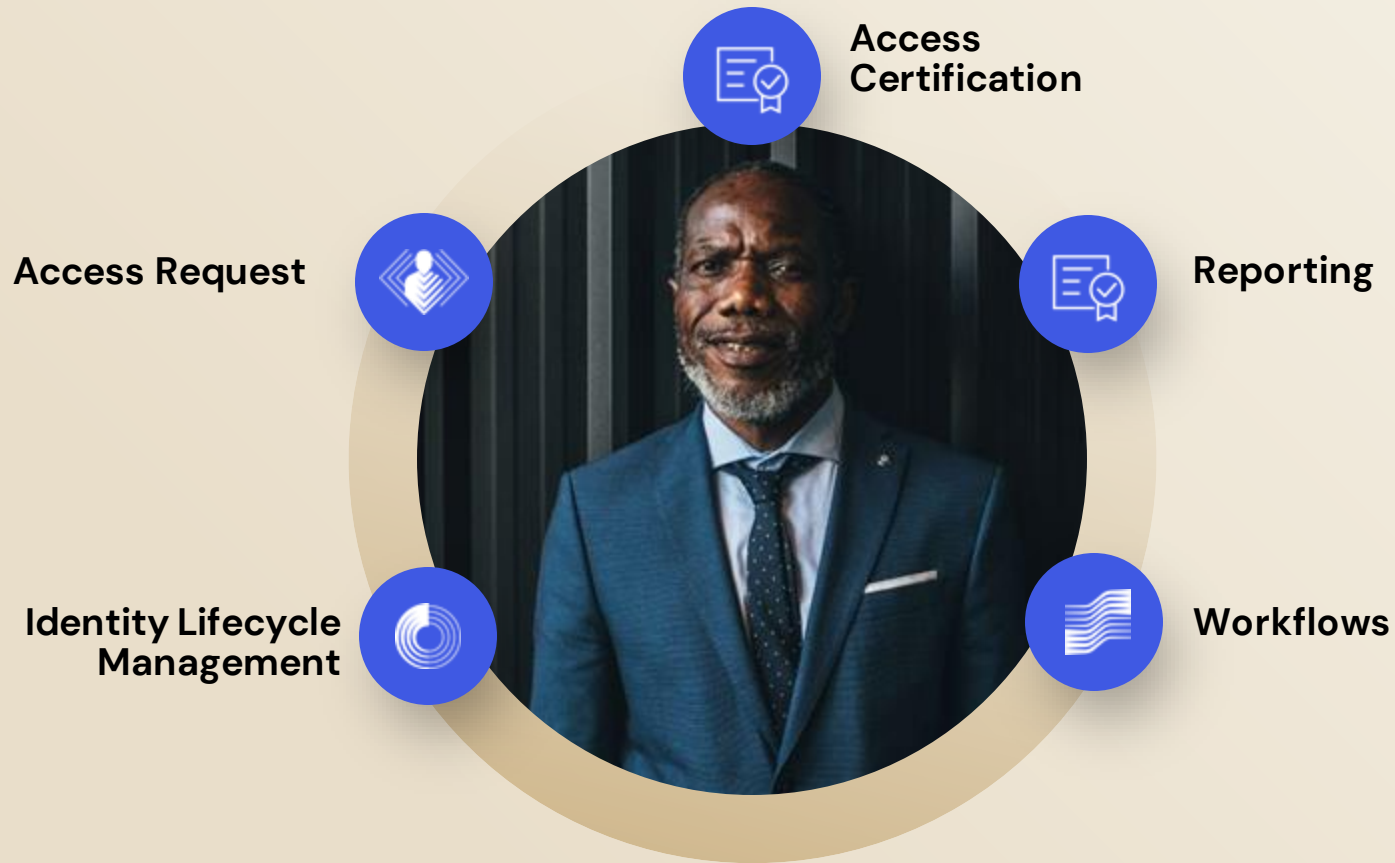
Okta Identity Governance: modern IGA



A unified IAM and Governance solution that improves enterprises' security posture and helps them mitigate modern security risks and improve efficiency.



Okta Identity Governance





Lifecycle Management



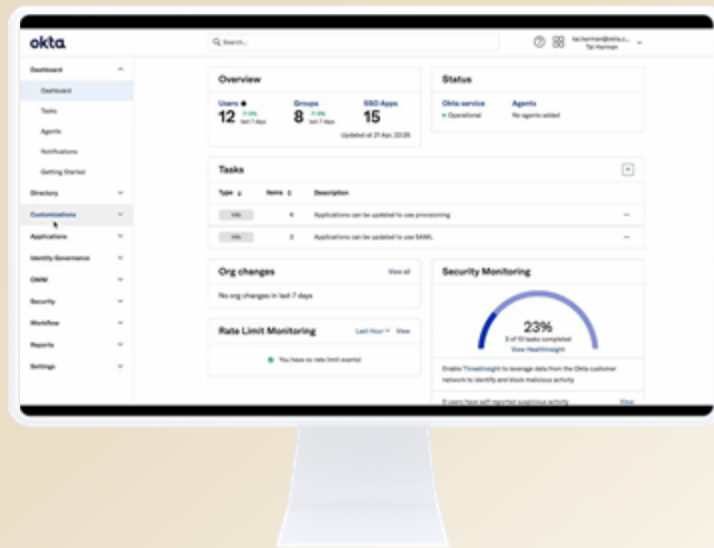
Access Request

- ML-driven Request Interface including Chatbots
- Control who can see and request what
- Support for time-based Access
- Modern customizable approval workflow builder



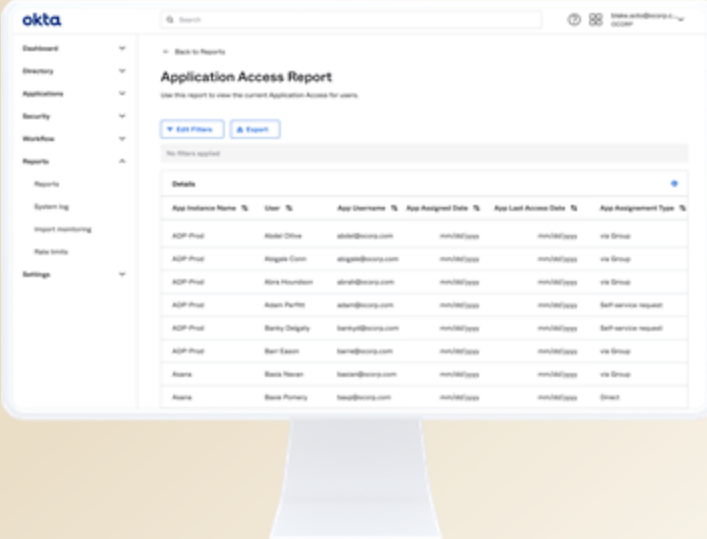
Access Certification

- Create and manage Access review policies to ensure right people have access to right resources



Out of the box reporting

- Query Okta to determine who has access to what resources, why access was granted, and when it was last reviewed in an audit campaign



The screenshot displays the Okta Application Access Report interface. The left sidebar contains navigation options: Dashboard, Directory, Applications, Security, Workflow, Reports, System log, Import monitoring, Role Inheritance, and Settings. The main content area is titled "Application Access Report" and includes a search bar, a "Back to Reports" link, and a "Use this report to view the current Application Access for users." Below this are "Edit Filters" and "Export" buttons. A message states "No filters applied". A "Details" section is visible, followed by a table with the following columns: App Instance Name, User, App Username, App Assigned Date, App Last Access Date, and App Assignment Type.

App Instance Name	User	App Username	App Assigned Date	App Last Access Date	App Assignment Type
ADP-Prod	Alder Drive	alder@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	via Group
ADP-Prod	Angus Conn	angus@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	via Group
ADP-Prod	Alex Houndson	alex@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	via Group
ADP-Prod	Adam Parke	adam@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	Self service request
ADP-Prod	Bobby Delgaty	bobby@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	Self service request
ADP-Prod	Bert Eason	bert@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	via Group
Axona	Beck Nevan	beck@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	via Group
Axona	Boris Pomeroy	boris@okta.com	mm/YY/ZZZZ	mm/YY/ZZZZ	Direct



Identity-based logic that connects apps across existing IT stacks

“When this happens”
Event



Okta assigns user to Salesforce

“If this”
Function



Is user on EMEA sales team?

“Do this”
Action



Assign EMEA territory

“Do that”
Action



Add user to EMEA Sales Channel and send a welcome message

Okta Identity Governance

Provides a significantly lower Total Cost of Ownership



Speed time-to-value

Immediate vs 6-12 months



Easy-to-deploy and maintain

Cloud Native, Easy-to-use and efficient



Lower Licensing Fees

Bundled with existing Okta Products



Root's compliance journey

Background

- Publicly traded tech-focused insurance company
- Clear mandate to not only protect Root and its customers, but to foster workforce productivity
- Needs to uphold the highest standards of data protection and regulatory compliance

Challenges

Growing access demands: With over 500 IT help desk tickets per month solely for access requests, Root faced the challenge of trying to parse employee requests and manager approvals on one system, while manually provisioning access on another.

Chasing certifications: Root's team found themselves spending over 100 hours annually to meet compliance challenges, diverting focus from driving business agility and larger technology-centric outcomes.



“It was like herding cats. It was a nightmare to manage and to get right. And this happens quarterly for all of our financially relevant systems. It was eating up a ton of time and resources for us and for our GRC partners.”

– Chaz Millfelt, Identity Engineer, Root Insurance



Root

Insurance Co

12

Critical systems

100+

Hours saved

0

Spreadsheets needed

Showcasing Okta Identity Governance



Demo



IGA's benefits beyond compliance



Getting identity management right

What meeting compliance with strong identity management does for your organization

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



Q&A

