Omada

Contextual Identity Governance

If identity access looks tidy on a chart but is chaotic in practice, the issue isn't authorization, it's context.

A regional manager, for example, may use an HR application to manage headcount in one role and a finance system to review cost centers in another. They may perform these duties in different contexts, within their line of business, or as part of a project team across multiple offices and countries. Each of those locations may have its own oversight rules, data residency requirements, and Separation of Duties (SoD) policies.

In everyday business, people and systems operate across duties, projects, and domains. When organizations ignore these realities, governance breaks down. Approvals lack business context. Certifications become checklist exercises. Excessive entitlements accumulate. Audit evidence is incomplete. The result is overlooked risks, over-permissive accounts, and costly compliance failures.

What is **Contextual Identity Governance?**

Contextual Identity Governance dynamically aligns access with real business context through a flexible, extensible model that adapts as roles and data domains change. It replaces static controls with intelligent governance that strengthens security and compliance as the organization evolves.

"Contextual Identity Governance" is Omada's unique approach to governing identities in the real world. It brings together a flexible identity model, analytics that understand how work gets done, and software-defined connectivity that reaches every corner of your business.

Overcoming the Constraints of Static Roles with Context-Rich Governance

Organizational charts capture static roles, but they rarely reflect how identities actually operate. Human and non-human identities shift across responsibilities, projects, and data domains every day. In most environments, closing the resulting identity governance gap means triaging email threads, opening ad hoc tickets, chasing business owners for justification, and editing entitlements manually one identity at a time.

Omada's contextual identity governance replaces these manual, fragmented processes with a clear, configurable, extensible model. Duties, projects, domains, data owners, and regional constraints are captured as first-class elements that drive identity decisions across requests, approvals, and certifications.

When someone requests access, the request carries its full context with it. This means it includes the business justification, the sensitivity level of the resource, and any applicable SoD (Separation of Duties) rules. Reviewers don't just see the request: they see the intent behind it, evidence-based recommendations, and suggested time limits, all in one place. Every policy check and decision criterion is automatically recorded for transparency and auditability. And when a project or responsibility ends, the system

automatically adjusts or revokes access in real time, ensuring access always matches current context. Because these identity to business relationships live in the Omada Identity Cloud model, rather than being scattered across spreadsheets or database files, teams can change course without reengineering. Adding a temporary role, launching a new project or applying regional oversight becomes a simple contextual configuration change made directly in the Omada Identity Cloud portal itself. Policies reference modeled objects directly, making decisions clear to reviewers, auditable for compliance, and adaptable as responsibilities evolve. The extensible model absorbs new duties and domains as they appear, keeping controls aligned with reality.

Modern IGA teams see immediate impact with faster reviews, fewer escalations, and the elimination of a buildup in privileges that are no longer needed or never used. With Omada, context-aware policies and real usage signals enforce least-privilege by rightsizing access continuously, with every decision producing audit-ready evidence as part of everyday governance.

Continuous Context, Real Time Trust

Contextual identity governance operates as an always-on control layer, enhanced by AI and analytics. As identities take on new duties, join projects, and interact with additional data domains, the extensible identity governance fabric updates constantly. Usage patterns, peer signals, and sensitivity signals enrich governance and entitlement decisions continuously without reengineering or spreadsheet drift.

Continuous context makes Zero Trust a reality. Each request is evaluated against current relationships, SoD rules, and real usage patterns. AI-driven recommendations clarify intent and highlight risk. AI-informed approvals and certifications prioritize identity profiles where exposure is highest. When the business purpose ends, access ends as well with audit-ready evidence captured automatically at every step.

Benefits for Every Stakeholder

- ✓ Security and risk teams see reduced privilege exposure and faster remediation.
- ✓ Auditors get a current, exportable trail because approvals, policy checks, context, and timestamps are captured as actions occur.
- ✓ Owners and managers can make decisions quickly because requests include the needed context.
- ✓ Employees and contractors receive right-sized access exactly when needed.

Why Omada

Selecting a contextual identity governance platform that can adapt as the business evolves is a critical requirement. Omada Identity Cloud provides a no-code, web-based approach that adapts as responsibilities, regions, and data platforms change. Each access decision is supported with recorded evidence, ensuring transparency and accountability.

With Omada, identity governance remains aligned with business change while maintaining security and compliance.