

# KuppingerCole Report

## EXECUTIVE VIEW

By **Matthias Reinwarth**  
June 08, 2021

## NEXIS 4

NEXIS 4 implements intelligent role and identity analytics together with strategic entitlement lifecycle management processes. As such, it provides the basis for dedicated, business-oriented Identity and Access Management (IAM) self-services within an organization either as a stand-alone solution or as a companion component to existing IAM infrastructures.



By **Matthias Reinwarth**  
[mr@kuppingercole.com](mailto:mr@kuppingercole.com)

## Content

<b>1 Introduction</b>	3
<b>2 Product Description</b>	5
<b>3 Strengths and Challenges</b>	9
<b>4 Related Research</b>	11
<b>Content of Figures</b>	12
<b>Copyright</b>	13

## 1 Introduction

Managing access to corporate resources remains an underestimated challenge for many businesses. Traditional approaches leverage the concept of roles and role hierarchy as an implementation of Role Based Access Control (RBAC). Alternative access management concepts extend and complement this approach by relying on the interpretation of attributes and context data for assigning access rights (like group memberships or individual entitlements) at admin time or for making access decisions within the individual applications at run time. So, augmenting authorization models like Attribute Based Access Control (ABAC), Policy Based Access Control (PBAC) and Dynamic Authorization Management (DAM) are becoming increasingly important.

Most organizations opt for an enterprise-wide role design that breaks down existing complexity into manageable roles. The definition, implementation and maintenance of an enterprise role model demands mature business processes and strong tool support. Providing these processes as user-friendly, easily modifiable, and traceable workflows is becoming increasingly important. However, comprehensive, and adaptable administration capabilities for all types of authorization management paradigms in a uniform manner are a key requirement in today's enterprises.

Furthermore, to benefit from existing expertise within an organization, it is also becoming more and more important to involve a variety of business stakeholders in the management, verification and maintenance processes of entitlements, their set-up and allocation. As processes become increasingly digitized and employees, teams and their areas of responsibility continue to specialize, while the processes required for managing authorizations and identities are also constantly changing. Their proper implementation calls for the involvement of many kinds of subject matter experts in different types of organizational units, for clearly defined and efficient administrative processes and for appropriate tool support.

Modern IAM environments thus require new management tools that can implement the described aspects of modern and user-friendly authorization management. This is done by providing a variety of capabilities along the lifecycle of both managing and assigning different permissions. The majority of IAM and IGA systems and suites are now equipped with functionalities that can be categorized as delegated administration. The breadth and depth of available functionality varies between the systems of different vendors, while the effort to be spent on implementing required functionality sometimes can exceed months. In general, typical user interfaces for this type of delegated administration are not necessarily aimed at non-technical, business users.

For a comprehensive analysis and modeling of roles, but also for the provision of all workflows for the implementation of role lifecycle management in companies, a small, highly specialized market segment exists as a complementary offer to traditional IAM systems. Dedicated entitlement management tools mostly originated as comprehensive role mining and identity analytics tools. Today's leading tools further demonstrate their capabilities by providing a wide range of services and capabilities between automation,

maintenance processes and governance.

This goes far beyond a unique approach to identifying initial role definitions, a point at which many initial role projects stop. Defining or reviewing the appropriate role portfolio with each role containing the right set of underlying individual entitlements for the required set of systems, infrastructures and applications must not be a one-time exercise. These serve as a framework for the administration, maintenance, and ongoing refinement of role definitions and for the assignment of the associated individual authorizations to identities.

## 2 Product Description

Nexis is a German software vendor based in Regensburg, Germany. They specialize in providing solutions and services around the analytics and the sustainable lifecycle management of enterprise and system-specific entitlements and their assignment to corporate users. NEXIS 4 (formerly branded as Nexis Controle) as their flagship offering is a highly specialized tool designed to operate as an add-on to an existing Identity and Access Management (IAM) infrastructure or as a stand-alone service with direct connection to target systems (e.g. AD or SAP).

The areas of application have expanded over time and the core pillars of its functionality can be described as follows:

- **Analytics and modeling for identities and their access.**

NEXIS 4 benefits from many years of experience in the design and continuous development of a technology for the analysis and modelling of authorization information which is unrivalled on the market. The focus in this area is more on the IT teams managing and analyzing authorizations while communicating results with selected stakeholders.

- **Lifecycle and governance functionality.**

By providing capabilities for the implementation of a complete, company-wide role lifecycle management, recertification, data quality and compliance processes can be embedded in enterprise processes and workflows, leveraging the expertise of departmental experts.

- **Platform for providing end-user IAG-services.**

With the dividing line between end users, business administrators and IT stakeholders becoming increasingly blurred, it is essential to provide user-friendly, well-integrated IAG services for all user groups.

NEXIS 4 covers, among other tasks, the areas of:

- role and identity analytics, including access governance
- attestation and periodic access recertification
- visual role modelling and role engineering
- intelligent and automated role mining and optimization
- entitlement management

- end-user friendly dashboards and self-services
- full role lifecycle management capabilities and
- identity intelligence and access clean-up.

The three-level structure mentioned above is also reflected in the logical structure of the product. As soon as information about existing roles, system authorizations and identities are available to the system (through data import or direct integration), it can be processed in NEXIS 4. The integrated analytics engine can identify, for example, dependencies and patterns, data quality issues or potential enterprise role candidates.

This data is leveraged as the foundation to implement workflows to manage authorizations (such as roles, policies, or groups) and their lifecycle. Automation and the extensive support of the affected stakeholders are the focus here. This also allows the assignment and verification of authorizations for users and user groups (access request and approval, transparency, and recertification).

There is no need to develop from scratch, rather the system provides more than 150 proven best practices workflows for a full role lifecycle management, including approvals, recertification and other standard business transactions that can be customized to individual needs. The focus is not on coding but on configurative changes. The tool offers free delegation paths, and multi-level processes for the implementation of, among others, any sequential and/or parallel approval processes, while means for escalation, e.g. after a defined number of working days are also available.

All workflows are configurable using graphical modelling and safeguarded by version control. The NEXIS 4 authorization concept allows workflows to be specified for individual user groups (data analysts, etc.). Runtime access to currently active workflows is possible by administrators and process owners.

With NEXIS 4 being the most recent update, the functional expansion of the tool from the analytics engine via the addition of workflows is being further enhanced by the addition of business user specific IAG services. These are freely configurable user interfaces that can be adapted to suit individual users and user groups. On the basis of so-called cards, i.e. individual configurable interface elements that can be added and configured via online visual modelling, dashboards and workflows are created for IT users and non-IT users. They can be managed using access control themselves, so that the same IAG service can offer different levels of functionality or detail depending on e.g., the qualification or increasing individual authorization.

The creation and maintenance of these services is based on a consistent no-code paradigm aiming at providing efficiently maintainable and quickly deployable workflows. This follows modern, efficient and agile approaches to decentralize the management of IAG by providing simplified and easy-to-understand services for business users in the departments and to be able to directly leverage the domain expertise in the organization.

In all other areas the product has been strategically developed and functionally extended as well. The analytics engine provides a broad range of grids for the automated and visually supported analysis and

modeling of authorization information (role or attribute based). This enables analyses on different levels, such as the association of roles to entitlements, of employees to roles or of meaningful employee attributes to system authorizations. Filtering of additional aspects (organizational information, employee attributes or role composition data) enables multidimensional analyses in terms of a drilldown to particularly relevant aspects including data analysis functions at resource level. Since NEXIS 4, time-based analytics have been introduced for further extending role management and governance capabilities. It is now possible to assess previous access control states and automatically react to certain changes in the past or the future (e.g., in scenarios where assignments, roles or entitlements reach their validity dates and respective workflows need to be executed).

All user interaction with NEXIS 4 is done through a web interface which can easily integrate with existing intranet platforms and portals. The comprehensive configurability of the IAG services also ensures visual integration into the corporate identity design of the company. Key NEXIS 4 functionality is externalized via an API while the system in turn is fully capable of integrating via API calls with adjacent systems. Since NEXIS 4, this, amongst others, also includes the possibility for preventive SoD checking which is integrated into third-party processes. NEXIS 4 can act as real-time policy decision point for external SoD queries.

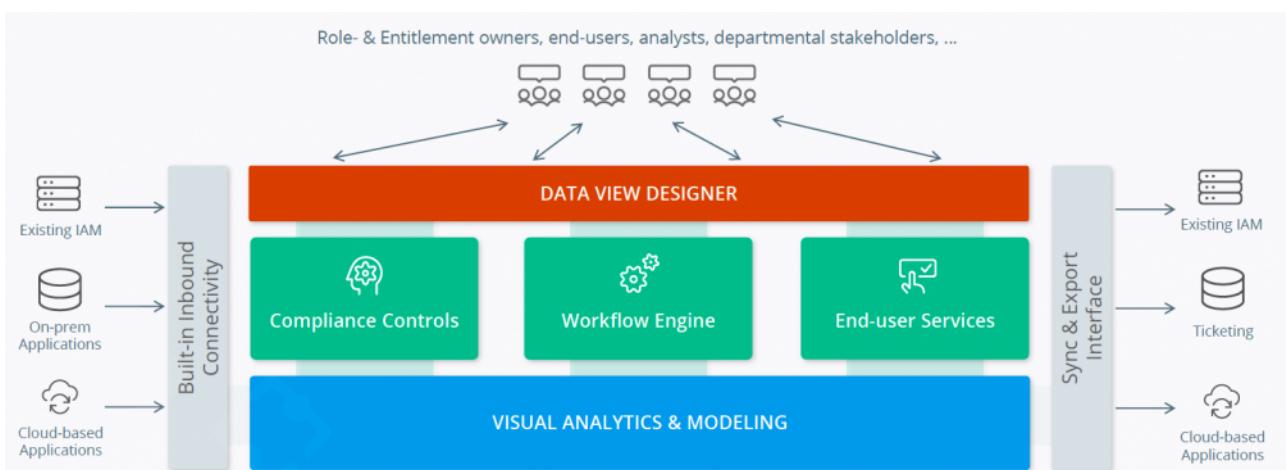


Figure 1: NEXIS 4 architecture (Source: NEXIS)

The basic concept of NEXIS 4 does not focus on the replacement of functionalities of an existing IAM system, but rather on complementing missing functionalities or the avoidance of cumbersome workarounds. NEXIS 4 can also be integrated with existing ITSM solutions (like ServiceNow) in case tasks or results need to be processed or approved within those systems.

NEXIS 4 can be deployed in various scenarios. A one-off clean-up or role modeling project might leverage the solution for a limited amount of time, with the analytic processes being executed once or for a few times aiming at an iterative improvement. Other usages include well-embedded, long-term enterprise-wide entitlement management processes and continuous compliance analytics. As such it can cover e.g., regular reporting, role lifecycle management, access approval and recertification processes, ongoing risk mitigation

activities and self-services which, e.g., can provide role owners constant control of their managed business roles via simplified dashboards.

NEXIS 4 installs as either a data center-based appliance or a cloud-based service. The consistent micro service architecture allows for adequate scalability. Scalability, fail-over and high availability can be achieved by establishing load-balancing across a set of NEXIS 4 nodes providing selected functionalities according to individual requirements.

To reflect the different application scenarios of the software, three modules are offered which provide different levels of functionality:

- NEXIS 4 Analytics Module: Provides the visualization, model simulation, role modeling along with policies and reporting
- NEXIS 4 Governance Module: Offers a visual workflow engine, the lifecycle management capabilities, recertifications and automated event trigger, integrated with the organization's CI
- NEXIS 4 Business Module: Offers the newly developed business dashboards, a modular UI-component designer, stakeholder services and access requests

### 3 Strengths and Challenges

NEXIS 4 is a highly focused one-of-a-kind product, deliberately designed to implement a clearly defined set of tasks. It complements existing IAM deployments with intelligent role analytics, role lifecycle and workflow management, identity intelligence for GRC and comprehensive access governance. The product can add value to a large variety of IAM deployments while easily integrating with existing systems. This is of even higher importance as role lifecycle management, including the required workflows, and analytics capabilities are often not adequately available from established vendors or quite limited even in leading IAM suites. The newly added IAG services make NEXIS 4 a powerful platform for swiftly and efficiently bringing tailored identity and access related functionality directly to target stakeholders. NEXIS 4 is truly a high potential product in a specialized IAM market segment with only a limited number of competitors.

Nexis is continuously expanding its market base. With an experienced, growing partner network, but also with its own expertise, Nexis serves an expanding range of clients in Germany, Austria and Switzerland (D/A/CH), but also worldwide.

The continuous development and product improvement, which is driven by both strategic and customer-oriented requirements, underlines the special position and quality of NEXIS 4 in the market. Nexis' ambitious strategy of a closer integration into enterprise processes, of a tight interaction with existing IAM landscapes and cooperation with established enterprise tools on the one hand, while at the same time maintaining its position as a technology leader in the analytics sector on the other hand, can be regarded as successfully implemented. The market visibility outside of Europe still deserves improvements.

Customer organizations looking for a product extending and augmenting their IAM-strategy in the areas of sustainable role management including user specific IAG services, workflows, access analytics and optimization, GRC and identity intelligence should consider evaluating NEXIS 4 as the technology leader in identity and access analytics and modelling for their purposes.



## Strengths

- Strong, efficient role lifecycle management, identity and access analytics and modeling capabilities.
- Powerful and adjustable workflow engine to leverage corporate subject matter experts know how.
- End-user focused IAG service platform offering detailed tailoring options for individual user groups.
- Fast deployment and versatile deployment scenarios, supported by adequate licensing models.
- Comprehensive best practice workflow and service library to jumpstart efficient rollout and configuration.
- Strict no-code approach for workflows and services with fast delivery of dedicated functionality to both IT and non-IT users
- Technology leadership around analytics and role lifecycle management.
- State-of-the-art service architecture for scalable, hybrid deployment models.

## Challenges

- European market first approach, but increasingly capable of delivering internationally through a growing, strong partner ecosystem.
- Visibility beyond the European market deserves improvement.
- Uncommon (but adequate) approach to augment and not to replace full IAM offerings needs to be communicated.

## 4 Related Research

[Whitepaper: Leveraging Your Organization's Expertise: Departmental IAM Services for the Business - 80429](#)

[Architecture Blueprint: Identity and Access Management - 72550](#)

[Leadership Compass: Identity Governance & Administration - 71135](#)

[Leadership Compass: IDaaS Access Management - 79016](#)

## Content of Figures

Figure 1: NEXIS 4 architecture (Source: Nexis)

## Copyright

©2021 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

**KuppingerCole Analysts** support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

**KuppingerCole**, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact [clients@kuppingercole.com](mailto:clients@kuppingercole.com).