KuppingerCole

VENDOR REPORT

by Martin Kuppinger | April 2013

Atos DirX

Identity, Security, and Risk Management as part of a broad solution portfolio. Industry focus and integration as reason for an IAM Business Case instead of pure technical solutions.

by **Martin Kuppinger**
mk@kuppingercole.com
April 2013

Content

Related Materials:

Advisory Note: The Open API Economy - 70352

December 16, 2011

Scenario: Understanding IT Service and Security Management - 70173

August 2, 2011

1 Executive Summary

Atos is one of the largest IT Service Providers worldwide, with more than 70.000 employees and global reach. Following the acquisition of Siemens IT Solutions and Services (SIS), the company changed its name from Atos Origin to just Atos. The company is listed on the Paris Stock Exchange.

This vendor report focuses on a specific part of the Atos portfolio, the DirX products. These are part of the Systems Integration division at Atos and within that division grouped into the solution area Identity, Security and Risk Management. While Atos primarily acts as solution provider with a set of services, this division develops its own standard software products for Identity and Access Management, branded as DirX solutions.

The special role of a division with its own product development has arisen as a consequence of the acquisition of SIS, where DirX also was one of the relatively few areas that developed standard software solutions. Based on the established market position of DirX products and the relevance of a solution portfolio in the area of identity, security and risk management, the decision of further acting as a product vendor also in the Atos environment was a logical consequence.

In December 2010, Siemens and Atos Origin announced that they would form a global strategic partnership. To create a new market-leading European IT company, Siemens AG then sold the business of Siemens IT Solutions and Services to Atos Origin in the summer of 2011. Thus, DirX products are now part of Atos, while the products and the structure of the product portfolio remain the same.

The considered product portfolio of DirX products is part of the overall Atos solution portfolio that is divided into 13 areas ranging from Adaptive Workplace to SAP Business Process Solutions. The DirX products also play a role in industry solutions by Atos and for Atos Managed Services. However, the actual products are classified as solutions within the area of Identity, Security and Risk Management. The DirX products in recent years at SIS, prior to its acquisition by Atos, had shown a very significant growth in the area of IAM (Identity and Access Management). Thus, the clear focus and the continuous development of the products have paid off.

Additionally, the industry-oriented and comprehensive solutions that have been realized by SIS using the DirX products for example, in the healthcare sector, eGovernment, in the utilities industry or convergence solutions for physical building and IT access - were important for that success. With the acquisition by Atos the distribution channels have become still wider. An advanced solutions industries portfolio is expected to become a result of the new structure. The company is very well positioned with a variety of existing customers, a global sales force and strong consulting support. We assume that the DirX product range within Atos can further improve its visibility and positioning in the market in the coming years and will have more success based on vertical solution offerings as well as in the area of managed services. Due to the strength of the product portfolio and the strong solution competence of the provider, we recommend including the DirX products of Atos in evaluation processes in IAM.

2 Research Highlights

- Clear positioning as part of one of the largest IT service providers worldwide.
- Significantly increasing number of customers.
- Solution-oriented portfolio beyond pure product offerings.
- Comprehensive, consistently improved solutions addressing the IAM core topics.
- Very extensive experience in IAM with a variety of very large reference customers.
- Related to the portfolio and the importance of the market, still a relatively low visibility in the market.
- Good coverage of the access governance market segment, but no specialized access governance solution available.
- Integration with strong authentication solutions.
- Only a few partners, but has its own powerful professional services group.

3 Customer Challenges and Industry Status

When looking at today's IT, it is driven by some major evolutions. Everything that is done in IT has to consider these evolutions.

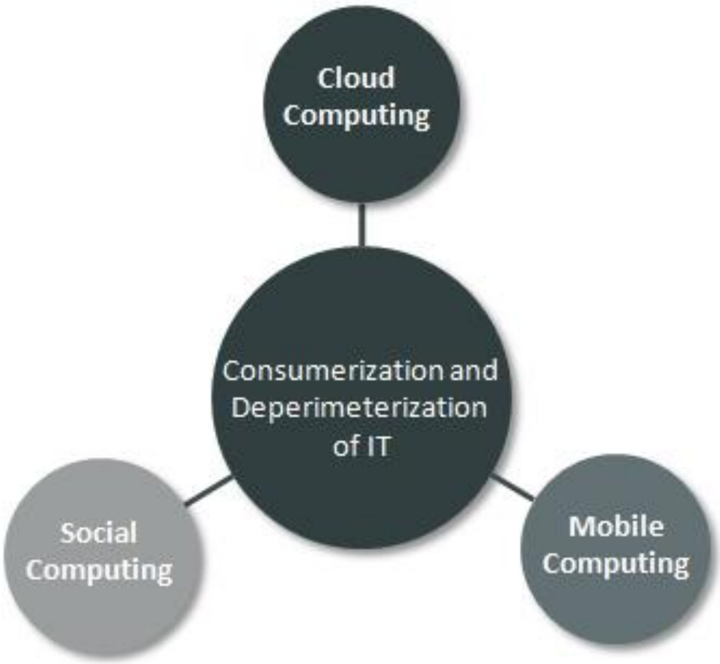

Fig. 1: The evolutionary areas of today's IT affecting every vendor's strategy.

Figure 1 shows these areas. One is Social Computing, i.e. a tighter interaction between individuals and organizations based on sharing information in some way – between publicly available information and a directed, controlled flow of information.

The second evolution is Mobile Computing, allowing access to a broad range of services via the Internet from different devices. This also pushes the accessibility of services, given that an increasing number of persons have device and network access available at virtually any point in time.

The third evolution is Cloud Computing, which in this context is not really new. It allows for using services that are located in the Internet to store and – willingly or unwillingly – share information with other parties.

All these trends affect IT fundamentally. The consumerization and deperimeterization of IT are logical consequences. Information technology (IT) is available to virtually everyone and virtually everywhere. It is not a business-to-business technology anymore, and hasn't been for quite a while. However, all three evolutions mentioned drive the consumerization of IT to a new level.

Deperimeterization is another logical consequence. Once formerly closed networks open up, there is no perimeter anymore. That not only affects the way Information Security has to be implemented, it also means that the borderlines between different organizations and between organizations and their counterparts in the form of individuals – customers, users, tenants, citizens, etc.- are not as clearly defined anymore.

Fig. 2: IAM Solutions have to help solving the "Identity Explosion" challenge.

Saying this, there is obviously a massive impact on Identity and Security. There are more persons (and thus identities) to deal with, not to mention the "Internet of Things," an exponentially growing number of devices. But even without the "Internet of Things", enterprises are facing the "Identity Explosion", where in addition to a limited number of employees, there are now a lot more identities--especially the clients, leads and prospects which number far more in many cases, as shown in Fig. 2. Managing security becomes a far bigger challenge than ever before. Thus, these major evolutions greatly affect what organizations have to do in Identity and Security.

3.1 Organizational Requirements/Customer Challenges

If one analyses these changes in the context of Identity and Access Management, Access Governance and GRC as a whole, then we see new challenges. Products that will cover future requirements must be able to deal with these challenges which involve, in particular, the following topics:

- Solutions must not be limited to the classic "on-premise"-IT environments, but also support services that run in the cloud.
- Solutions must be designed to support all types of users, including employees of business partners and customers. This requires sufficient scalability, but also the presence of rules that go beyond the view of the staff only. One example are people who on the one hand are employed at an insurance company and on the other hand also work as freelance insurance brokers. Of course, they should not be allowed to approve the contracts they have sold.
- Solutions have to protect information (such as documents and personally identifiable information – PII) efficiently, especially when they are propagated beyond the enterprise or if they are stored outside the company.

In addition, the well-known challenges should not be underestimated. These include, with regard to the considered product category, in particular the following areas:

- Companies are faced with a growing number of regulatory requirements, which require a precise control, audit and traceability of the management and the status of permissions across system boundaries.
- Administrative processes around the identities and their access privileges must be simplified.
- Users must get easier access to the request and recertification of access entitlements to be able to use these functions efficiently. The same applies to other functions in the relevant areas.
- Regarding auditing, it is necessary that requirements are supported in a simpler and more efficient way and to consolidate information of specific solutions for monitoring of, for example, access permissions or certain systems into a holistic view.

The requirements for Access Governance, IAM and GRC in total have increased significantly in recent years.

3.2 Industry Status

This development is also reflected in the market. In recent years, several trends to watch are:

- There is a separate market segment of Access Governance products. However, most of the products in this market segment have expanded using their own connector technology thus providing enterprise provisioning functionality as well.
- On the other hand, vendors from the field of enterprise provisioning have extended their products to increasingly integrate Access Governance functionality to meet new requirements.
- Auditing capabilities are relevant not only at the technical level of IT; they also must provide information in a form prepared for the business users. They must support the consolidation of information as well.

This, together with the modified structure of the IT operations with cloud services as an alternative form of service delivery and the increased governance requirements, results in the need to fundamentally adapt IT structures.

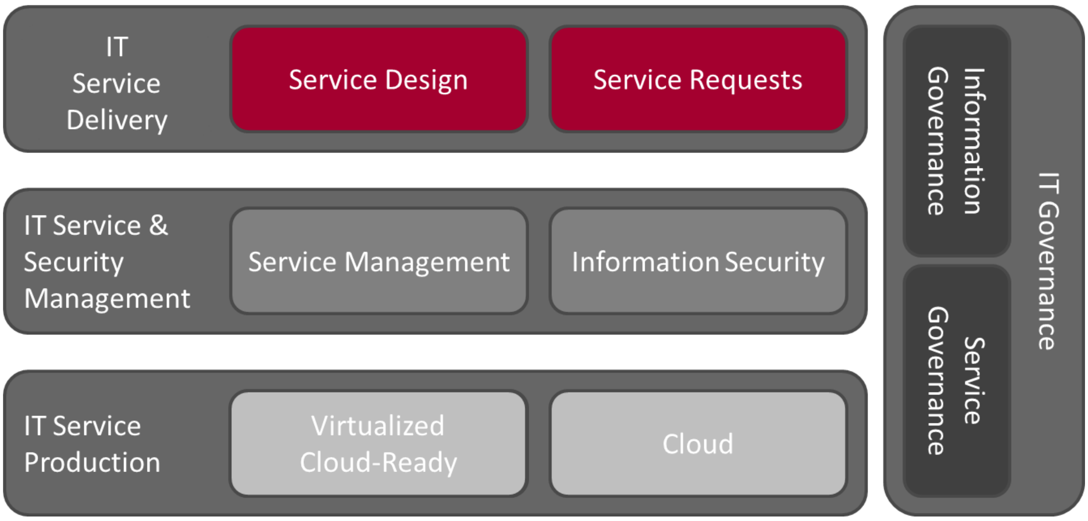

Fig. 3: The KuppingerCole IT paradigm as a design guideline for IT infrastructures.

This development is reflected in standardized form in the KuppingerCole IT paradigm, a guideline for the design of IT infrastructures. Enterprise Provisioning and Access Governance are here central elements as core components of Information Security in the area of IT Service & Security Management, but also for Information Governance within the larger field of IT governance.

Access Governance is also an important component in the area of Business Service delivery, i.e. the provisioning of IT services in a form that is appropriate for the end user. Here Access Governance comes into play with its focus on access request management and the recertification functions for end users.

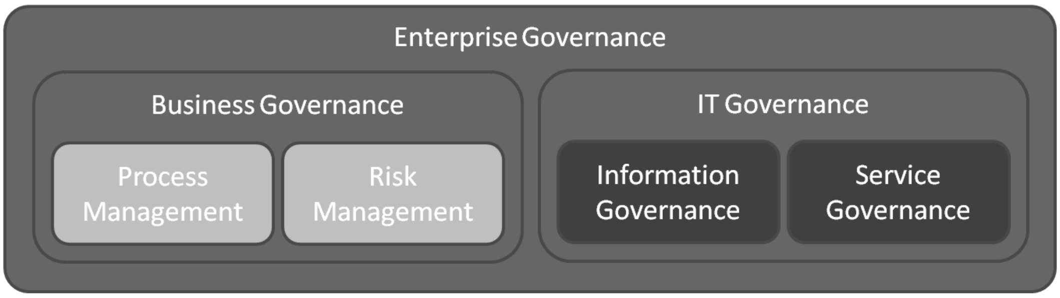

Fig. 4: GRC infrastructure must consolidate Enterprise GRC-and IT GRC requirements.

In addition, IT governance itself is gaining momentum, which in turn must be integrated with Business Governance to support a full Enterprise Governance concept. The consolidation of different audit information into an overall vision has a central role here, because both process governance and risk management are based on consolidated information delivered by IT governance solutions.

3.3 Mapping of Challenges/Status

Overall both the vendors and their client companies have recognized the fundamental developments and are beginning to implement them. In particular, however, with regard to the "Identity Explosion" and the inclusion of external users, such as business partners and customers, both sides still are facing significant development needs. The same applies to a holistic view of Enterprise Governance with IT governance and Business Governance linked closely.

In addition, both the customers and the industry are still evolving, so that future innovations are to be expected, but also customers will have to correct the path they once took.
Vendors must therefore carefully analyze the major trends and align their development with it, particularly as regards the broader focus beyond employees. This requires innovations, but creates at the same time new opportunities for the providers to position themselves as market and technology leaders and innovators in the area of Access Governance, IAM and GRC.

4 Vendor and Ecosystem

The IAM solution portfolio with DirX is part of the *Identity, Security and Risk Management* offering of Atos, which is in turn associated with global solutions. These are separate pillars of the overall Atos portfolio, in addition to the industry solutions (vertical markets) and outsourcing.

Atos thus is primarily a solution provider, not a product vendor. This corresponds to the structure that SIS already had, where the DirX solutions were part of a solution portfolio and have played an important role, for example, in creating special solutions for healthcare. Accordingly, the division has always been focused on providing holistic solutions based on the specific requirements of the customer, which goes beyond the purely technical solution. DirX solutions for IAM and Access Governance have benefited considerably from the acquisition of SIS by Atos Origin, according to KuppingerCole, so that in addition to the established Siemens clientele also the Atos Origin customers directly can be addressed and an even wider range of solutions will be offered. Clearly, therefore, the company should benefit from the currently strong and likely to be growing demand for solutions in this area.

4.1 Product portfolio (IT)

Atos achieved a turnover of around €8.5 billion - calculating the acquisition of Siemens IT Solutions and Services (SIS) pro-forma - in 2011 and has approximately 74,000 employees in 48 countries. This represents approximately a doubling of sales compared to SIS and a further advanced global presence. Concerning the SIS-sales, it should be noted that over 75% were obtained from outside of the Siemens group.

The DirX products are important within this portfolio for different industry managed services solutions. Comprehensive information on the structuring of Atos is provided on the website of the company. The services are divided into Consulting & Technology Services, Systems Integration, Managed Services and the so called High Tech Transactional Services to support business processes. Special solutions for the energy sector and for healthcare are added with Atos WorldGrid. SIS was historically very strongly represented in both areas. All sectors are relevant also for the delivery of solutions using DirX technology.

Atos has also been the worldwide IT partner of the Olympic Games in London. Here, issues of security also play a very important role, which underlines the competence of the group in this field, where the DirX products are also allocated. Specific strengths are those projects where IAM core solutions are integrated with other security products. These combinations include, for example, converged access solutions for building and IT access with a smart card, the integration of biometrics solutions, or the implementation of public key infrastructures (PKIs). Here, Atos can also continue to rely on a very comprehensive range of technologies, products, and problem-solving skills. Important industries also include eGovernment in addition to the areas mentioned before such as utilities and health care. Basically Atos is active in virtually all industries and IAM solutions based on DirX technologies can deliver value for all industries.

4.2 Portfolio in the area of IAM and access governance

The product portfolio of Atos in terms of Identity and Access Management with DirX focuses on four products:

- DirX Identity: Identity and Access Management-core solution for role-based provisioning and access governance
- DirX Access: Access management with a focus on Web access management and Federation with broad standards support
- DirX Audit: Central analysis of identity-based audit data
- DirX Directory: Directory Service

In addition, other solutions are offered by Atos based on these products and integrated with other products.

Beyond the pure products, Atos focuses on integration in horizontal solution portfolios (Atos solutions), and industries. So, also integrated applications of IAM are available. Such a solution strategy is pursued in this consequence by almost no other vendor in the IAM and GRC market and could increasingly become a competitive advantage for the company. This is even more true given that IAM and Access Governance as of now, especially due to the massive increase in compliance and audit requirements, have become core components of various solutions and are increasingly understood by the customer.

4.3 Services

As one of the largest service providers in the IT market worldwide Atos can handle even the most complex projects. The company also has a large number of dedicated IAM consultants, which exceeds the total number of employees of several of the smaller vendors in the area of IAM and access governance. This is a clear advantage when compared to many other providers in this area. Atos can compete here also with the leading IAM and access governance providers. As one of the largest outsourcing providers, Atos also offers IAM solutions as managed services and cloud services.

In addition, the service employees in many cases have specific industry expertise. This is a result of the focus on solutions and also the history both of the Siemens group and SIS as Atos itself. These industry skills are not to be underestimated for the successful implementation of projects.

A disadvantage of the Atos construct is that there are only a few external partners (e.g., Siemens Enterprise Communications, T-Systems). However, these partners gain significant revenue. Given that Atos has a sufficient size in itself, this point is significantly less critical than with smaller providers. Due to the competitive situation of Atos to other system integrators we also assume that partnerships for DirX products in the future will be the exception. There are partnerships today especially in the technology sector, which is also mandatory for the integral solutions by Atos.

4.4 Company and Financial Data

Atos came about through the acquisition of Siemens IT Solutions and Services (SIS) by Atos Origin. The new company is economically sound at a significant profit and at acceptable high operational margins. The company has a free cash flow, which is considerably higher than the debt. It is assumed that the economically solid company can keep its huge customer base and expand it, despite these times of economic turmoil.

The market situation for the IAM products is positive. SIS had a significant number of customers and could increase both the number of customers as well as the amount of sales considerably in future years. In the years since 2005, the number had more than doubled. It is also remarkable that at least 25% of the customers are located in North and South America. This is a very significant value for a

European manufacturer. We assume that Atos can continue the positive development of this business segment.
Notably, the IAM division of Atos is better positioned with respect to both the number of customers and growth rates as many in the market assume. Atos clearly is to classify amongst the leading vendors on a global scale in that market segment.

5 IAM and Access Governance Portfolio

In the area of IAM and access governance, Atos especially focuses, in addition to the mentioned solutions, on core products for the area of IAM. That includes a noticeable expansion towards a stronger support of specific access governance requirements in the product of DirX audit as well as by significant functional enhancements in DirX identity.

5.1 Products

The current core products in this area are the DirX products already mentioned. DirX Directory is a directory service with LDAP and x.500 support, which is designed in particular for scenarios that need reliability, high scalability and performance. DirX Directory is an established product, which has already been in the market for many years.

DirX Identity was created several years ago through the combination of DirXmetaRole and DirXmetahub, the solutions for role-based identity management and synchronization of identity data. The product has been developed consistently over the years and has established itself as a provisioning solution on the market. In recent versions, many features were added, especially for access governance. Among other things the changed and improved user interface for access via the Web, the addition of self service, and the built-in functions of certification as a further component of access governance are concepts worth mentioning.

The portfolio has been supplemented for quite some time by DirX Access. This is a modular server for access management and Federation, which supports both Web and SOA applications. Atos has designed this product so that new features can be integrated flexibly.

With DirX Audit, Atos has further expanded the IAM offer towards access governance and function-specific SIEM. This broadening of the portfolio is worth noting in the context of an increasing importance of analysis functions. However, DirX Audit is not an access governance solution in the narrow sense with support, for example, for recertification, request permissions or Enterprise Role Management. These functions are provided by DirX Identity and also expanded in that product. DirX Audit enables the central evaluation and analysis of identity-based audit data including a condensed representation in a dashboard. It is, thus, more part of a new area of access governance, which is often referred to as Access Intelligence. However, it also can be considered as a specialized SIEM solution related to access risks. These products cover the core areas of IAM and access governance. Atos can refer to a broad solution portfolio in that space. In contrast to some other vendors, Atos lacks a specialized access governance solution. However, this fits with the trend where vendors either strengthen the access governance functionality in their identity provisioning core products (as Atos does) or add provisioning functionality to access governance solutions. The functions can be found in the Atos portfolio in DirX Identity and to some extent in DirX Audit and should be significantly expanded in upcoming releases.

5.2 Market Segments

The following table provides an overview of the Atos product portfolio within the market segments for IAM and Access Governance defined by KuppingerCole.

Core Market	Market Segment	Atos Products	Comments
IAM	Directory Services	Yes	
	Meta Directory Services, Provisioning, Delegated Administration	Yes	Fully supported, including Meta Directory functionality.
	Virtual Directory Services	No	
	Enterprise Single Sign-On	Partners	
	Web Access Management and Web Single Sign-On	Yes	
	Strong Authentication and Password Management	Yes, plus partners	PKI, biometrics, smartcards, integrated solutions. Basic functions for Password Management on basis of the Windows password synchronization.
	Identity Federation, User-centric Identity Management	Yes	Full support for relevant standards.
	Privileged Account Management	Limited	Administration of shared user accounts such as administrators and superusers.
	Information Rights Management	No	
	Platform-specific Access Management	No	No specific solutions for system environments such as mainframes or UNIX
GRC	Access Governances	Yes	Features integrated in DirX Identity, additional support in DirX Audit.
	SIEM, Auditing, Logging	Partially	Comprehensive support for auditing in the IAM products, including re-certification and central analysis of identity-related audit data with DirX Audit. No full SIEM support, but good support for specific IAM and IAG requirements.
	ERP GRC	No	
	Enterprise Role Management	Yes	Comprehensive role management features in DirX Identity.

Table 2: Atos products and the IAM/GRC market segments defined by KuppingerCole.

The table illustrates once again that Atos covers the essential areas of the IAM market with its DirX products and, in some cases, via partners. The fields not addressed in the IAM market are mostly niche topics, which are covered mainly by specialists or are still evolving as in the case of IRM (Information Rights Management). Furthermore, Atos can always integrate third-party products into its own solutions to provide the functionality required by the customer.

5.3 Strategy

The DirX products are clearly positioned in the context of the solution portfolio of Atos. The company consistently works on further development and puts these products in many solutions. Thus the fundamental situation of the strategy assessment for Atos does not change compared to the previous assessment for SIS.

As already mentioned SIS did not and Atos does not first and foremost position themselves as a software provider for standard solutions. However, for their solution focus, their own products are of great importance because they are essential for the fulfillment of compliance, auditing and security requirements. Here, access to their own products offers clear advantages for the realization of solutions.

The DirX division of Atos has significantly increased the pace of innovation in the area of IAM in the past few years. Focusing on products and additional standardized solution scenarios are useful from our point of view. It is assumed that gaps in its product portfolio will be filled through partnerships and their own developments. We believe that Atos is well positioned. Substantial risks due to any uncertainty concerning their future strategy are thus not relevant from our point of view.

6 Rating

KuppingerCole as an analyst company regularly does evaluations of products and vendors. The results are, amongst other types of publications and services, published in the KuppingerCole Product Reports and KuppingerCole Vendor Reports. KuppingerCole uses a star rating to provide a quick overview on our perception of the products or vendors.

Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are as well understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet the customer requirements. In mature market segments, the status of the industry and the KuppingerCole expectations usually are virtually the same. In emerging markets they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in the portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management and discontinuation of the each product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context it means the degree in which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree in which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to insure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy) for more information about the nature and state of extensibility and interoperability.

Usability —accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, overall we have strong expectations regarding well integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes and breakdown. This will create openings for attack and failure.

Thus when Kuppinger Cole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of highest importance. This is because lack of excellence in any or all of these areas will lead to inevitable identity and security breakdowns and weak infrastructure.

For Atos, the following ratings apply:

Security ➚	Overall, a very good solution with consistently implemented security models. The architecture is well thought out. Purchased components by third-parties were consistently integrated, so that the security challenges in such situations were addressed. Security patches are delivered in a defined manner to customers. Internal access is controlled for the core functionality via the same mechanisms that are also used for the management of access permissions in other systems. There is a high degree of flexibility with regard to these mechanisms. While auditing can be externalized (among other things based on DirX Audit), XACML is not supported for the control of access permissions in the system. The latter is however only of limited relevance for this product category.

Functionality ➚	The products largely meet the expectations of KuppingerCole in their overall point of view, although there is potential for improvement. For individual products, there are still weaknesses: for example, Atos DirX Identity as regards the flexibility of recertification. However, Atos has shown in projects that it is able to implement highly complex solutions for customers. Enhancements in the product are included in the road map, so that even here a positive assessment can be granted. The products have a defined position in the market and with the strong solution focus of the company a potential for achieving a unique selling proposition, even while there is still a lack of visibility. Compared to other products in the market all major functional areas are addressed, but to slightly varying degrees. The functionality promised by the manufacturer will be provided.
Integration ➚	The integration of the various DirX products is good. However, there are still older products with legacy components, which might represent a special challenge in the operation. A good integration at all levels is achieved with joint surfaces and the consistent use of web services. Overall, a positive evaluation is awarded. It is positive to mention that Atos has implemented the integration of purchased functions such as in DirX access to a high level and consistently.
Interoperability ➚	With a consistent focus on providing web service interfaces the products are rated positively in this category. For all major products of the portfolio, such interfaces are provided and documented. Most standards are supported in the field of Identity and Access Management.
Usability ➚	Atos has completely revised its user interfaces in the past few years and unified them. A high degree of consistency is available for end users. In the administrative area, there are even greater differences through a number of different approaches for the administration. However, the products in this area are generally good. In the field of the installation procedures, the products could be simpler to use and provide greater integration. Since implementation is typically done by consultants, this is of limited relevance.

For KuppingerCole Vendor Reports, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the particular market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus active participation in standardization initiatives adds to the positive rating of innovativeness.

- **Market position** – measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor takes into account the vendor's presence in major markets.
- **Financial strength** – even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with massive risks for the execution of the vendor's roadmap.
- **Ecosystem** – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

For Atos, the following ratings apply:

Innovativeness ➚	Due to the latest innovations, only a slightly positive evaluation will be awarded here even if the active involvement of Atos in standardization initiatives could be pronounced. The focus on providing solutions is positive, while the pure functionality of the product is good, but Atos is not an innovative leader in that area.

Market position ➚	Atos is not a perceived market leader for IAM and Access Governance despite its strong market position in different industries and countries. The company operates worldwide and has available resources and reference customers in all major markets.
Financial strength ➚	Atos is listed on the stock exchange and shows positive numbers and a solid financial basis.
Ecosystem ➔	Atos has a limited partner infrastructure, which is caused by the structure of the company. There is broad support in the area of technology partnerships. Despite the ability to solve customer's requirements with their own resources, only a neutral rating is given due to the relatively small base of external partners.

7 Summary and Recommendations

Atos is according to KuppingerCole amongst the most powerful vendors in the area of IAM, with a comprehensive product portfolio and a very large number of reference projects, including many projects with very large numbers of users.

7.1 Business cases

With its solutions, Atos can support a number of business cases. The following are exemplary cases that show only a small range of options but which are particularly interesting from our perspective here:

- Integrated solutions: one of the strengths of Atos is to be able to offer integrated solutions, where IAM is a part of an overall solution.
- Federation: In this area Atos DirX Access is extremely well positioned and powerful.
- SOA security: Federation for SOA-based applications becomes increasingly important, and therefore also here is an increasingly important field for Atos. Atos is also strongly positioned here with DirX Access.
- IAM for SAP environments: Atos continues to have one of the best SAP integrations in the IAM market. Thus it appears to be an interesting solution for heterogeneous environments with large SAP infrastructures. In addition, Atos can offer strong solutions in this area.
- IAM for healthcare environments: in collaboration with the Siemens healthcare sector, the DirX products were integrated with hospital solutions and integrated solutions for supra-regional infrastructures. Atos itself possesses a large Healthcare Division.
- Overall concepts for strong authentication: combining the Atos DirX products with solutions for strong authentication, Atos is very well positioned in this area.

It is noteworthy that this is just a sample of possible use cases. Atos can provide very suitable solutions with its portfolio in "classic" application scenarios covering Identity Provisioning, Access Governance, Single Sign-On and Federation.

7.2 Products

In this area, Atos appears very well placed. In addition to its entrenched products it has established itself in Access Management and Federation with DirX Access. Moreover, it has consistently developed DirX Identity, where Atos focused on expanding the functionality after doing major changes at the platform level in the past few years. DirX Access also shows that Atos has adapted well to modern product architectures. The J2EE-based architecture of DirX Audit is further evidence that Atos consistently has pursued this strategy. We assume that Atos can further keep the innovation ability shown in the past few years.

7.3 Services

Here, Atos is exceptionally well positioned. Only a few players in the market such as IBM have larger service units. That also applies to the area of IAM, where Atos has a considerable number of its own specialists. The constraints in the partner area are therefore acceptable.

7.4 Recommendations

Overall, Atos is one of the most interesting suppliers especially in the extended area of IAM including Access Governance functions. The company has a high degree of solution expertise and offers in the important areas a powerful product portfolio. It is also clearly strategically positioned. This will not change at Atos as compared to the earlier situation at Siemens according to the expectations of KuppingerCole.

We assume that Atos can significantly improve its visibility and positioning in the market in the coming years on this basis and will have increasingly more market success based on offers for vertical markets. In particular for the mentioned business cases, we recommend including Atos DirX products in the evaluation processes. In addition, we recommend considering DirX Identity in the evaluation of strategic central platforms for IAM.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports 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 leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Am Schloßpark 129
65203 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com