Do you know your users?

An AdNovum IT Consulting White Paper, October 2012

AdNovum

Who we are

AdNovum has been designing, implementing, maintaining and updating sophisticated software solutions for companies and government authorities for almost 25 years now. We pass the knowledge and experience acquired in the course of our project work on to our customers with our consulting services. We offer support for all complex IT undertakings, irrespective of manufacturer or product. Our offering embraces all solution levels – from technological issues and process design, right through to IT strategy consulting.

Identity and access management (IAM) is one of AdNovum's core competencies. AdNovum has evaluated, devised and implemented IAM solutions for many renowned customers in the public and private sectors. The scope of this work includes an analysis of existing user accounts, the conceptual design of access control solutions, user and privilege management and project implementation and support.

http://www.adnovum.ch

The authors

Peter Gassmann has been in charge of IT Consulting at AdNovum Informatik AG since April 2012. He joined the company in the summer of 2010 as a senior IT consultant and identity architect. Before that, he worked for Sun Microsystems for 10 years, where he was also involved in identity management. At AdNovum, Peter Gassmann gives customers advice on all aspects of security and identity and access management and he also manages projects in this field.

Thomas Zweifel, who joined AdNovum in 2006, graduated with a Master of Science ETH in Computer Science and a MAS MTEC at the Swiss Federal Institute of Technology in Zurich (ETH). In his capacity as senior software security engineer, technical project manager and IT consultant, he has been involved in numerous projects with AdNovum, particularly projects focusing on IT security, identity and access management and IT strategy. Thomas Zweifel was previously self-employed for six years. He now advises and manages projects in these fields.

Do you know your users?

Data theft and illicit transactions are among a company's most critical risks associated with IT. It is important to know what each user has done. Traceability and reproducibility are not only essential for auditing, but must also be ensured in the event of undesirable incidents, such as data theft. User accounts with appropriate access rights are frequently used for this. In the context of governance, risk management and compliance (GRC), it is therefore advisable to establish systematic control of user accounts and access rights. This document explains and highlights influencing factors, risks and solution approaches associated with user accounts.

A personal user account that represents the identity of a user in an application is usually needed for applications in the business environment. This personal user account offers a means of assigning access rights to an identity for control and traceability purposes. The access rights define the actions that may be carried out by a user in the application. As soon as a user logs into an application with his account, the application knows the identity of the user who has logged in and can therefore check whether he has the authority to perform each requested action. To the same extent, the user performing an action and the circumstances under which the action was performed can be recorded and audited.

Factors that influence user accounts

As shown in *Figure 1*, user accounts are subject to many influencing factors, the majority of which can be directly affected by the company that controls the business applications.

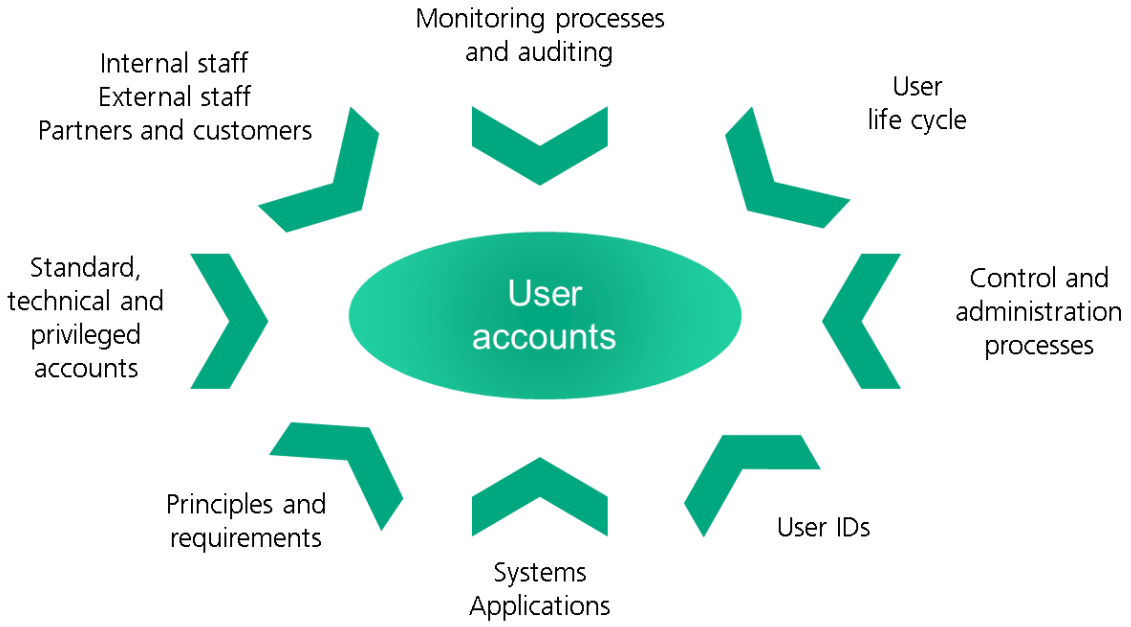

Figure 1: Factors that influence user accounts

These influencing factors are explained in the sections below. Some of these factors, e.g. the control and management processes, can be defined and controlled by the company. As far as the factors that cannot be influenced directly are concerned, a means of identifying possible risks and enabling reliable control and traceability must be found.

Processes associated with user accounts

A user account is governed by a life cycle that encompasses its generation, modification, activation and deactivation and finally the deletion or archiving of the account. The user account is influenced by a multitude of events during its life cycle. These include, for example, the granting or withdrawal of access rights for the staff member responsible for the account, depending on his function and duties. *Figure 2* shows an exemplary life cycle for an internal member of staff.

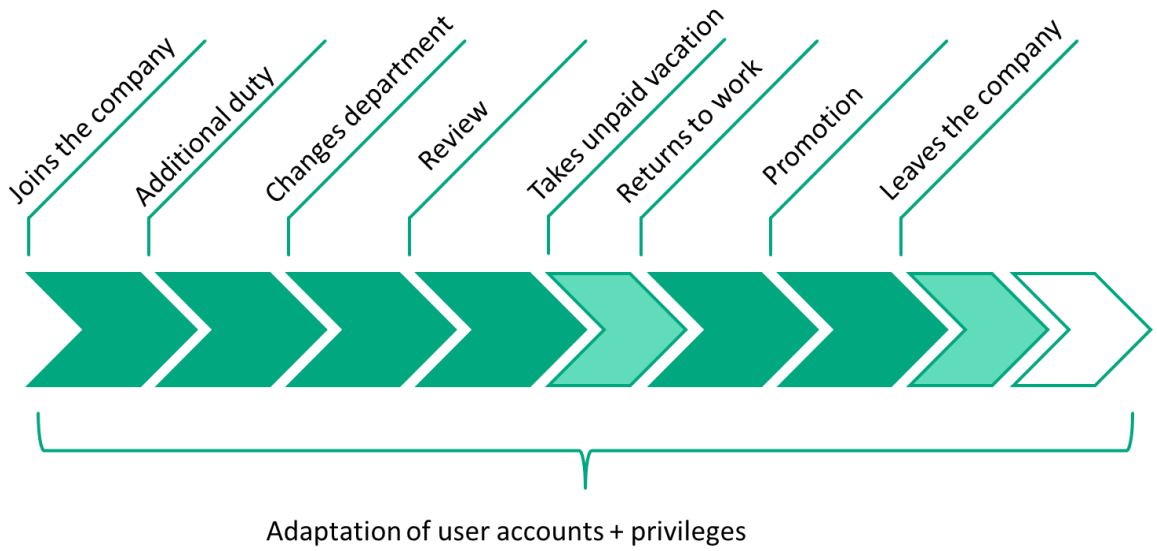

Figure 2: User life cycle of a member of staff

The personnel management processes for regular staff members are closely meshed with the life cycles of their respective user accounts within the company. The starting point of each one is the date of joining the company and mutations, promotions, reorganizational measures and other changes may occur along the way. The final stage in the life cycle is the staff member's departure from the company. Based on the personnel management processes, the authorization processes have been clearly defined and established in the majority of companies. Such processes are rarely clearly defined or monitored for non-personal accounts, however, irrespective of whether the accounts concerned are privileged, technical, test or training accounts.

Life cycles are not always clearly defined for non-company personnel either. In many cases, although the ways in which a user can be created or imported have been specified, no procedures have been established that specify the way in which regular audits are to be conducted or designate the person responsible for locking a user in the event that he leaves a third-party company so that his external account needs to be disabled or deleted as a result. In this context, it is not always clear which data sources can be used for non-company users or how these are to be maintained. This means that, under certain circumstances, a customer relationship management (CRM) tool may contain more information concerning partners and customers than the identity management tool. The timeliness and quality of available data is frequently inadequate in this respect.

The user management and authorization processes must involve all of the applications in which user accounts or access rights are needed. The complexity and the time and effort involved in process implementation and ensuring consistency between the required and actual status increase with the number of applications that have their own user management system.

No access rights – no problem ...?

Under normal conditions, members of staff have a direct interest in being granted the access rights needed to perform the work assigned to them. They continue to make positive efforts to obtain authorization until the access rights have been granted. This process works very well in many companies because it can take a

reactive and passive form to a certain extent: the user applies for authorization, the application is validated and access rights are granted. If anything goes wrong, the user will get in touch.

But will the user get in touch if he has been given too many privileges? Or if he no longer requires access to a particular system? Hardly. Because this does not present a problem for the user. He can perform the work assigned to him in spite of having too many privileges. Apart from anything else, the user may not even be aware that he has been granted too many privileges. Trainees are a good example to illustrate a situation where too many privileges are granted: in many companies, trainees work in one department after another in order to obtain a general overview of the various work processes and parts of the company. They need the access rights required by the department in which they currently find themselves in order to do the work assigned to them and gradually accumulate all of the privileges that a member of staff in the company can possibly be granted, in spite of the fact that the department-specific access rights are no longer needed once the trainee leaves the department concerned. Therefore, an internal change is regarded as being a good reason to check and correct privileges as a matter of principle.

Too many privileges – risks and costs

If a member of staff has too many privileges, this may lead to a situation in which defined processes are bypassed. That means, for example, that someone may authorize his own orders in spite of the fact that he should not be able to do so. Some of the most famous cases of fraud in recent years – particularly in the world of banking – can actually be attributed to a member of staff being granted or having acquired too many privileges and therefore being able to undermine the control procedures. Staff members who control several user accounts and those who are able to log in with a technical account represent a particularly high risk. Many companies are still finding it difficult to even determine whether too many privileges have been granted. It is not always even possible to unambiguously assign all of the accounts to the pertinent member of staff. The situation is exacerbated by privileges that are only described in technical terms and cannot be unambiguously correlated with the business context.

Fraud is not the only risk, however. There is also a risk of data being destroyed deliberately or unintentionally. Privileged accounts are often used to perform bulk operations which, in some cases, act on all of the data in a system without any restrictions being imposed. Manipulation errors occur from time to time in the course of day-to-day operations, which means that these accounts increase the risk of vast quantities of data being affected by a single error. The improper or unauthorized use of technical accounts also gives rise to considerable risks as comprehensive access rights are often granted to such accounts for synchronization purposes, for instance.

Special attention must be given to those users who have been granted remote access to the company infrastructure. These also include external service providers, where access information is sometimes shared between several users for remote support purposes, for example.

If nothing else, unnecessary access rights can also be a direct cause of extra costs: some applications are licensed according to the number of registered users. This means that unnecessary costs are incurred by every user account that is no longer needed. In this respect, costs can also be reduced by actively monitoring the use of such applications and promptly deactivating unused access facilities.

Ensuring traceability and reproducibility

Apart from controlling applications by means of selective allocation of access rights and privileges, particular importance is also attached to traceability and reproducibility. If something goes wrong, it must be possible to use the audit logs to establish which actions were performed by whom as a minimum requirement. In this case, the user ID for the account used to perform the action provides a link to the member of staff concerned, who should be called to account if need be.

Most diverse types of account

Different types of user accounts may be needed within a single application. The account types vary according to user group and purpose. The associated risk profiles and processes also vary accordingly. The risk profiles give the application operator an indication of how likely it is that a particular type of account will be used in an improper or even criminal manner. *Table 1* below gives an overview of the various types of account.

Type	Description	Risk profile
Standard account	Personal account for day-to-day operations	Normal risk as long as a life cycle is defined from creation through to account deletion. This being the case, personal accounts are usually well monitored, which means that every action can be assigned to a specific individual.
Privileged personal account	Personal account with additional or special privileges, e.g. for administrative tasks.	Greater risk due to extended access rights.
Privileged non-personal account	Account with additional or special privileges, e.g. for administrative tasks.	High risk as the account cannot be assigned to a specific individual. Therefore, responsibility is not clearly defined and traceability and reproducibility are not ensured.
Technical account	Account used by one application to interact with another one.	Higher risk as the account cannot be assigned to a specific individual and the implementation of such standard policies as password changing is virtually impossible.
Training account / test account	Account used for training or test purposes. Ideally used in test systems only.	Low risk as long as the test environment is isolated. Higher risk if the test environment is linked to production systems as such accounts are usually used over and over again and are therefore impersonal.
External account	Account of an individual who is not directly employed by the company. Often used by external personnel, suppliers or partners.	Higher risk as the implementation of life cycle processes for external individuals is more complicated and more susceptible to error.
Customer account	Account of a customer	Higher risk if the configuration allows access to internal systems as the implementation of life cycle processes for customers is more complicated and more susceptible to error.

Table 1: Overview of user account types

Some of the account types in the table above are unambiguously assigned to specific individuals. These include the standard accounts, the privileged personal accounts and the accounts for customers and external personnel. Personal accounts may be adapted when the person concerned enters and leaves the field of reference for the application as long as the information is available on time.

Apart from the personal accounts, there are also technical accounts, which systems and applications can use to access other systems and applications. The application does not make any distinction between technical accounts and the accounts of normal users. They are not used interactively, however, and it is typical for the means of authentication or credentials to be stored in the systems. When these are stored in systems, it is often impossible to use such protective mechanisms as regular password changes for these accounts because the responsibility is not borne by a single person but is shared by the members of a team, which

means that the scenarios for non-personal accounts have to be taken into consideration. Unauthorized read-out is another risk associated with storing credentials in a system, which can give rise to account abuse. The risk potential increases to an even greater extent as a result of the fact that technical accounts are also used in scenarios with higher-level access rights.

Training and test accounts are set up when training new members of staff and when new applications are introduced. A test system is used, where available, to avoid any operating errors in the production system while conducting exhaustive tests on new applications. Such accounts may also be created and used in the production environment depending on the configuration, system architecture and availability of test systems. Like personal accounts, these give rise to a higher risk level as traceability and reproducibility can no longer be assured.

Apart from the types of account mentioned above, there are also user groups, who use external accounts and are not within the company's sphere of influence: they include the personnel of other companies, such as suppliers, partners, corporate customers or end users, who require access to the offering company's infrastructure.

Access via external accounts often takes place less regularly and less frequently, making it more difficult to implement security guidelines. Apart from this, companies do not want to scare end users off by imposing rules for complex passwords and frequent password changes. There is also the possibility that strong authentication requiring additional devices is out of the question because of the costs involved.

Privileged accounts

Special access rights are needed in order to use administrative functions in an application. So-called privileged accounts are therefore often created for administrators with the motivation that such accounts are to be used selectively and consciously for administrative tasks, which cannot be performed with a normal user account.

As far as these privileged accounts are concerned, a distinction must be made between personal accounts and non-personal accounts, which may potentially be shared by several users: although there is a higher risk associated with privileged personal accounts by virtue of the additional privileges, it can be ameliorated by means of regular reviews of the need for such privileges and additional protective measures, such as password stipulations or the use of strong authentication, such as certificates. This is only possible to a limited extent when it comes to privileged non-personal accounts, such as *root* in a Unix-based system, however. This gives rise to a higher risk in general, which must be examined in greater detail and evaluated.

The account types described above offer a means of understanding and grouping the various risks that exist within the user management and access control environment. All of these types of accounts and the corresponding groups of users must be taken into consideration in order to completely control and consider the risks associated with user accounts. The formulation of appropriate measures must allow for the differences between the various user groups and be geared to their specific needs and requirements.

Risk minimization principles

There are various basic principles that can be adopted to keep user accounts in conformity with the business processes and regulations to the greatest extent possible. Adherence to these principles helps to reduce the risks to a minimum.

The principle of "least privilege" or least access rights is the most important of these. According to this principle, a user should only be given those privileges which are absolutely essential to that user's work. This means that access rights should not be granted to all employees indiscriminately, but according to strict criteria that take the business processes and the current roles of the respective staff members into account. This also includes the withdrawal of privileges as soon as they are no longer required, as is the case in the example for trainees given above.

The separation of functions and duties, known as the "segregation of duties", is another important principle: here too, the roles in the processes which may not be performed by one and the same person must be defined on the basis of the business processes. This offers a means of ensuring that an individual person cannot circumvent important control procedures just like that. The 4-eyes principle is another one associated with control and monitoring. This dictates that certain stages in the process have to be confirmed or acknowledged by more than one person. This principle also makes it difficult for an individual staff member to undermine the processes.

The principles are summarized in *Table 2* below:

Principle	Description
Least privilege	A user is only granted those privileges that are essential to the user's work.
Segregation of duties	The duties required to complete a task must be shared by different individuals, making it difficult to abuse privileges.
Keep it simple	Simple security mechanisms and concepts that are easy to understand reduce possible errors.
Open design	The security of a system must not depend on the secrecy of the security mechanisms' design – i.e. no security through obscurity.
Fail-safe defaults	Every access is prohibited unless access rights have been explicitly granted.
Complete mediation	Every access attempt is always validated before access is granted.
Psychological acceptability	Additional security mechanisms must not make the use of a system more complex than it would be without the security mechanisms.

Table 2: Important basic principles

These principles apply to the design of the user management and access processes to the same extent as to the design and implementation of applications.

Challenges and solution approaches

The risks associated with erroneously granted privileges may be addressed by means of appropriate implementations of the principles described above. The principles can only be implemented if the functions and roles for the business processes have been defined in the applications, along with the necessary privileges. This means that the role played by every user can be laid down within the framework of the processes, whereby one user can play several roles. Controls and checks are not possible unless the application-specific roles have been defined. This is where the first challenge is encountered, as the necessary documentation or knowledge is frequently either lacking or incomplete, particularly for older applications. The retrospective compilation of documentation may be very expensive and time-consuming where applications have been in service for a very long time.

When developing roles with respect to the abstraction layer for application privileges, attention must be given to ensuring that the roles are intuitive and indicate technical values in a manner that is easy to understand, where applicable. This is essential because the privileges should not be granted by computer scientists, but by senior personnel in the specialist departments, who understand the specialist background and the requirements. At the same time, attention must be given to ensuring that the role model does not become too complex and that employees do not find it difficult if not impossible to obtain the access rights required to deal with business-related and business-critical processes in good time.

Furthermore, in some cases, there is no central body that defines a unique user ID that a member of staff can use for all of the applications. Use of a personnel ID may not function in the desired manner because of the user group or account type. This leads to a situation in which it is not possible to unambiguously assign each user account in the systems to a specific member of staff. In other cases, different sets of rules apply to user IDs, particularly where legacy applications are concerned. That means that it is necessary to first establish an integrated (correlated) view that enables an assessment as to whether an employee's actual privileges are in accordance with the rules.

If the processes, functions and roles for the applications have been defined and granted for the first time, a regular checking process – automated if possible – is needed, which ensures that the user has the correct privileges – and only those. It is often the supervisor or manager, who knows, defines and assigns the roles to his personnel within the framework of the processes. The supervisor or manager should therefore also be involved in the checking process. When checking required and actual privileges, it is important to ensure that the actual privileges are actually analyzed at the point where they are called up by the application. It is not unusual for alleged actual privileges in a central directory to be supplemented by local "additional privileges" in the application itself and such situations must be taken into consideration or, better still, avoided.

Apart from the actual content and order of the checking process, the frequency of checking must also be defined. That means that an assessment of the risks associated with the privileges must be carried out for every application. The challenge here is to identify and assess the risks as this requires an understanding of the technical aspects of both the application functionality and the business processes and data involved. The risk assessment can then be used as the basis for a decision regarding the frequency and nature of the checks. This task is further complicated by the fact that the "segregation of duties" principle, in particular, has to be checked and enforced across applications.

A company's employees run through certain processes automatically and this makes the personnel system an expedient source system. It provides a natural starting point for the definition and, ideally, automation of process steps for an employee's accounts on the basis of the employee's life cycle within the company. However, the personnel system is unable to supply any input for the accounts of external users. Additional processes must be defined and implemented here, as non-company personnel and suppliers' employees are also subject to life cycles. As already mentioned above, a customer relationship management system could provide a useful means of managing contact information concerning partners and customers in this respect. Alternatively, the possibility of a direct-real-time interface to partner companies by means of a federated system can also be investigated.

If a privileged account is assigned to a member of staff directly, it is then a personal account and presents the same challenges as a normal account. The main challenge presented by privileged non-personal accounts, and technical accounts in particular, is the identification of an individual who is responsible for such an account. An assessment of the necessary privileges is by no means a trivial matter as the basis for the assessment may be hidden in the logic of the application.

As far as remote access is concerned, particularly in the context of support provided by a supplier, the associated risks may be reduced considerably by enabling the access facility for a limited period, coupled with a recording of all actions taken.

Use of the identity federation approach, e.g. based on the SAML standard data format, can make complicated central checking and synchronization processes superfluous as such systems support distributed user management processes.

Risks related to technical accounts, in particular, can be reduced by the use of token-based authentication.

Enforcing governance, risk management and compliance (GRC)

As far as GRC is concerned, user accounts and privileges constitute an important element in the enforcement of company-specific rules and standards. Rules, which are based on risk assessments and oriented to compliance with regulations, determine the users who are allowed to work in specific processes and the privileges granted to them. The implementation of a completely automated enforcement of such rules is not always feasible, which means that manual checks are usually required as supplementary measures. The effort and expense involved in defining the rules, developing the infrastructure and processes and enforcing the rules vary according to the complexity of the IT landscape and the GRC requirements.

Procedure model

The following procedure has proven successful in transforming an unknown, uncontrolled user account situation with the associated risks and costs into a defined, verifiable situation:

1. **Analysis of the actual current status:** An analysis of the current status of the processes relating to applications and user management. An analysis of the current status of privileges and access rights for all applications. The necessary course of action can be derived from the results.
2. **Requirements:** A definition of the requirements to be met by the processes, applications and data, including a classification of risk.
3. **Checks:** Performance and establishment of checks, prioritized according to risk.
4. **Correction:** Errors identified in the course of the checks are corrected in the applications. This particularly includes the removal of unnecessary privileges from the accounts.
5. **Establishment of a central user management system:** A central user management system supports the processes and provides a central unit for the collection of all user information.
6. **Establishment of a role-based authorization system:** A role-based privilege management system supports the performance of reviews, creates transparency and enables automation of the authorization process taking the various types of account into consideration.
7. **Policies:** Automatic policies and controls, particularly with respect to compliance with the *segregation of duties* principle, can be established on the basis of the central user management system and the role-based authorization system.

The most important success factor for a sustainable and acceptable user management infrastructure is the involvement of the specialist departments, as this is an issue that is not purely oriented to IT. The specialist departments must become involved at an early stage to ensure that the teams, supervisors and managers are able to contribute towards the definition and control of the authorization processes. The company management's backing for the project is another decisive factor, as it would otherwise be extremely difficult to implement such a concept successfully.

Conclusion

User management is subject to constant change: new applications are introduced and existing systems are upgraded or the configuration is modified. Organizational structures are altered, companies merge, business processes are adapted and areas of responsibility are redefined. All of these changes lead to a situation, in which the detailed aspects of user and privilege management are mutating all the time. The processes for user management and monitoring must allow for these mutations as well. User management and the procedural steps described above add up to much more than just a simple project. AdNovum has helped various companies establish a successful, controlled user management system with the necessary infrastructures. The individual stages were broken down into sections and processes that were manageable for the company and the staff, while establishing areas of responsibility that ensure continuous further development and improvement. An investment that pays off: these companies know their users.

Headquarters
AdNovum Informatik AG
Roentgenstrasse 22, CH-8005 Zurich
Phone +41 44 272 6111
E-mail: info@adnovum.ch

Bern office
AdNovum Informatik AG
Erlachstrasse 16b, CH-3012 Bern
Phone +41 31 952 5858
E-mail: info@adnovum.ch

AdNovum Singapore
AdNovum Singapore Pte. Ltd.
72 Anson Road, #07–01 Anson House
SG-079911 Singapore
Phone +65 6536 0668
E-mail: info@adnovum.sg

AdNovum Hungary
AdNovum Hungary Kft.
Kapás utca 11–15, H-1027 Budapest
Phone. +36 1 487 5000
E-mail: info@adnovum.hu