The Business Case: A Central Element of IAM Investment

In this white paper, we make the case for a company-wide project to modernize your Identity and Access Management (IAM). These provide an excellent basis for fully demonstrating the benefits of an advanced IAM program.

Today, IAM is the central element in the management of corporate networks – and at the same time one of the biggest risk factors. The number of identities has multiplied due to the increasing digitalization and integration of various stakeholder groups, from employees to suppliers to end customers. Modern IAM approaches offer enormous potential for saving various types of resources and preventing security breaches.

Below we explain why a business case is one of the four most important elements of an IAM program.

Table of contents

1. Introduction

This document provides you with a comprehensive guide to developing a business case for Identity and Access Management from both a business and a risk perspective.

In the first part of this paper, we look at the phases necessary to build an IAM business case. These include vision development, goal setting, and typical business and risk drivers. The second part describes risk and business metrics that are used for the economic and professional assessment of an IAM investment.

Figure 1:
Problem/solution matrix of similar logistics companies from the IAM perspective

1. Challenges

- No central view of an identity in terms of permissions
- Different lifecycle processes for internal and external identities
- Logistics stream with many different 3rd party identities
- High degree of self-developed apps
- No central authentication and authorization
- Increasing complexity of infrastructure and access points

2. Scope of topics

- Automation of employee life cycle process
- Access according to the least privilege principle
- Connection of hundreds of apps and systems
- Audit-proof reporting / full traceability of who has what rights, and why
- Governance and risk control functions for compliance fulfilment

3. Potential solutions

- Professional conception and technical realization of the identity management processes in coordination with service managers, CISO, HR and IT departments in different countries.
- Implementation of authorization workflows
- Implementation of audit and reporting requirements
- Consultation with customers of the platform and technical connection of target systems

4. Advantages

- Traceability, recording, and acceleration of employee entries, changes, and exits
- Governance functions to minimize risk
- Automated connection of target systems
- Fast replication of approval processes
- SaaS: costs for operation, maintenance, security, upgrades are eliminated

2. Developing a business case for an IAM investment

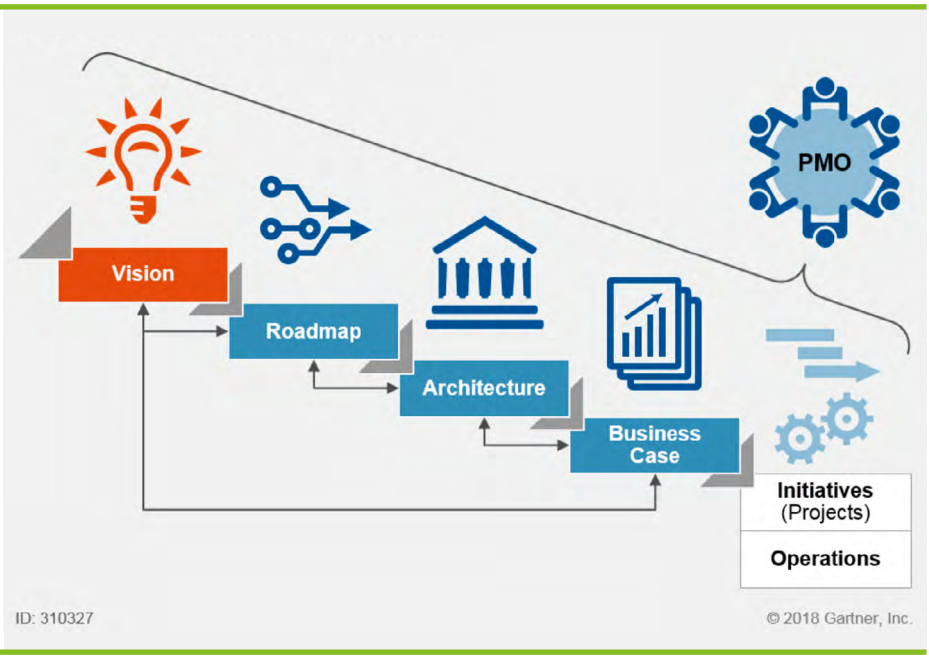
Security and risk management executives often have difficulty obtaining adequate funding for investments in IAM functions. IT leaders need to present a compelling business case that demonstrates the program's alignment with business needs and provides metrics to define success.

Security and risk management managers should:

- Demonstrate that the scope, objectives, and priorities of the IAM program reflect a working consensus among stakeholders by involving them in the development and approval of the program vision.
- Align all IAM program objectives with business drivers, and articulate these aims in clear language (no acronyms or technical jargon).
- Define precise risk metrics that align with the KPIs/KRIs to justify the need for change, and define the conditions under which success will be measured against these metrics.
- Communicate the risks of program implementation, and demonstrate commitment to risk management based on the planning of program initiatives.

The business case is one of the four most important elements of an IAM program, along with the vision, roadmap, and architecture. Its purpose is to justify the financing of the company's IAM strategy, which requires both resources for specific projects and personnel for ongoing operations. This funding is the foundation for a successful IAM program. Figure 2 shows the different phases for building such a program.

Figure 2:
Components of an IAM program according to Gartner, 2018



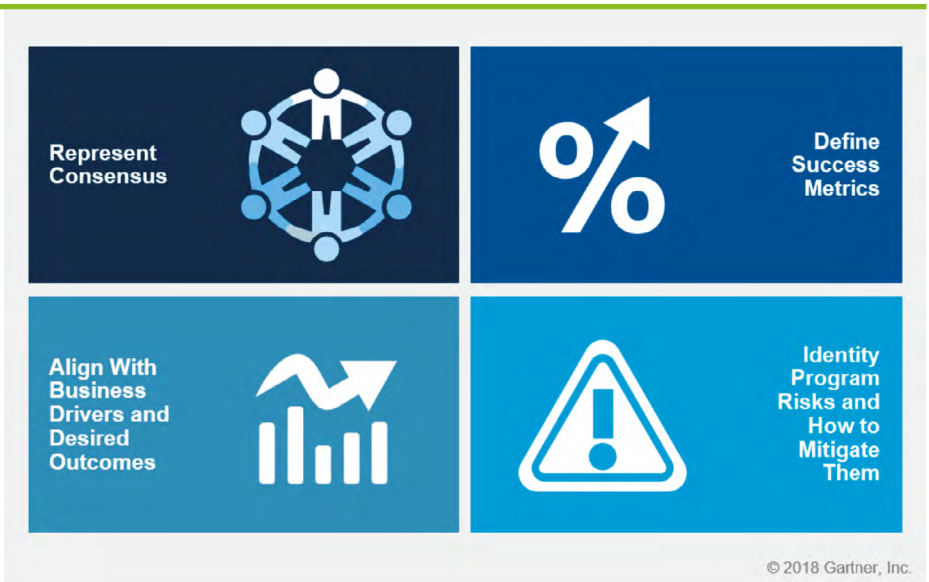
Source: Gartner (May 2018)

Without adequate funding throughout the program – not only in the first year but also in subsequent years – it is almost impossible for an IAM program to make progress in meeting stakeholder needs.

How can IAM leaders develop a compelling business case that will increase the likelihood of the organization adequately funding the IAM program?

Figure 3 shows four rules that IAM leaders should follow to develop a compelling IAM business case

Figure 3:
Four important rules for developing an IAM program according to Gartner, 2018



Source: Gartner (February 2018)

With regard to these rules, we will go into more detail on two points that should sharpen an initial view of IAM and show why it is necessary to take a closer look at the topic of IAM right now:

1. Vision, goals, and business drivers
2. Definition of key performance indicators

The other two rules ("consensus" and "risks of an IAM program") as well as the IAM aspects "roadmap" and "architecture" will not be discussed in this white paper.

3. Vision and goals

Implementing a modern, scalable Identity and Access Management solution to secure the digital identities of employees, partners and machines and to promote their collaboration. The new IAM solution meets regulatory requirements and better controls security risks. This is achieved, among other things, through secure authentication options, an optimized identity lifecycle and the allocation of authorizations according to least privilege. The advanced IAM program also helps to manage the logistical flow of goods across platforms.

Example of an IAM vision for a logistics company:
Implementing a modern, scalable Identity and Access Management solution to secure the digital identities of employees, partners and machines and to promote their collaboration. The new IAM solution meets regulatory requirements and better controls security risks. This is achieved, among other things, through secure authentication options, an optimized identity lifecycle and the allocation of authorizations according to least privilege. The advanced IAM program also helps to manage the logistical flow of goods across platforms.

Clearly defined goals and services, as well as a tightly defined framework for planning and monitoring them, are success factors for any IAM project. This in turn requires close cooperation between experienced staff, both at the user and the implementing IAM vendor. It is therefore important to ensure that all data and objectives are agreed upon and understood by everyone involved in the project before implementation begins. Any subsequent adjustment will unnecessarily prolong the project, both in terms of time and budget.

Example of an IAM goal formulation:
The objectives of Identity and Access Management are to ensure trust, integrity, and availability of systems and data. IAM should make it possible to identify, authenticate, and authorize users for access to important resources according to the least privilege principle. Other goals are to meet compliance requirements, reduce the risk of data theft, improve operational efficiency of the life cycle, and reduce staff costs as well as IT expenditure.

4. Business and risk drivers

Identity management has become business critical and the challenges of secure access are now more complicated than ever. They range from a huge increase in applications used (on premise and in the cloud), the trend towards hyper-outsourcing and non-linear career paths, agile transformations leading to cross-functional workplaces, and the rapid shift to a virtual workforce. As a result, many companies have implemented IAM systems to control complex IT infrastructures with dozens or even hundreds of systems and applications and thousands of accounts and access rights.

Certain business and risk drivers are often the reason why an IAM system is built. They take on a strategic importance to demonstrate to non-business decision makers how certain drivers influence risk and which factors have an impact on security, governance and authorization processes.

The following influencing factors are common arguments to justify the purchase of an IAM system:

- Shifting the security perimeter: Digital identities are now at the center of the security strategy. Previously, the focus was on network security.
- Hybrid infrastructures: Data migrates to the cloud.
- The definition of "unauthorized access" shifts away from the systems and focuses on the data. In other words, an authorized user can gain unauthorized access.
- Cyberattacks are on the rise: Hackers are seeking out "orphan/dormant" credentials of identities and using their credentials to penetrate systems and grab data.
- 81 per cent of data thefts are due to poorly protected or overly broad permissions.[1]
- Growing demands from industry standards and regulation in relation to data protection, privacy and compliance.
- No central view of the permissions of identities. Result:
  Identities have permissions without the "least privilege" principle.
- Managing compliance requirements, such as least privilege, becomes more difficult with increasing size. Remote workers need timely access, but managing permissions across multiple tools increases both operational costs and compliance risk.
- The number of access points is increasing steadily, increasing the complexity of the IT infrastructure and the risk of breaching compliance.
- Authorization allocation and revocation in the course of an employee or partner lifecycle still take weeks or days instead of hours in many companies.
- Customer Experience Paradigm: Employees and third party partners expect a fast, secure, personalized and easy login and access experience

The Federal Office for Information Security (BSI) is the German cybersecurity authority and the shaper of secure digitalization in Germany. BSI guideline ORP.4.2 describes risk factors and dangers when an IAM system is missing or insufficient.

1 Verizon, 2019 Data Breach Investigations Report https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

The following specific threats and vulnerabilities are of particular importance for the ORP.4 Identity and Authorization Management building block:[2]

1. Missing or inadequate IAM processes
If identity and authorization management processes are inadequately defined or implemented, there is no guarantee that access is restricted to the necessary extent, thus violating the principles of "need to know" and "least privilege". The administrator may not receive information about personnel changes, and, as a result, a former employee's user ID is not deleted. This person can then continue to access confidential information. It is also possible that employees who have been transferred to a new department retain their old authorizations and thus accumulate extensive rights over time.

2. Lack of central user access deactivation
In institutions, employees often have user access to various IT systems, such as productive, test, quality assurance or project systems. These are usually located in different areas of responsibility and are often managed by different administrators. Under certain circumstances, this leads to a situation where the same and unique user ID is not used on all IT systems and there is no central overview of the user accesses on the individual IT systems. In such a scenario, it is not possible to deactivate all user accesses of an employee in one step in the event of an attack or password theft. Also, in this scenario, when an employee leaves the institution, it is not possible to disable all accesses in one work step.

3. Inadequate management of access rights
If the allocation of access rights is poorly regulated, this quickly leads to serious security gaps, e.g. through uncontrolled growth in the allocation of rights. When introducing identity management systems or audits, it often turns out that different people in different organizational units are responsible for assigning authorizations. Under certain circumstances, this leads to users receiving authorizations on demand or, conversely, only obtaining them in unnecessarily complicated ways. On the one hand, missing authorizations can hinder daily work, and on the other hand, authorizations can be granted without a requirement, thus posing a security risk.

Summary: Why does it pay to invest in a centralized IAM solution?

- IAM solutions are used to reduce and control access risks, and to provide compliance for auditors.
- IAM reduces security risks, fulfils governance rules, and decreases process costs.
- A robust IAM program becomes the cornerstone of an organization's privacy and security strategy.
- Orchestration of policy-based user identity management and access control during the access request and certification process, also known as provisioning, fulfils legal requirements.
- The BSI recommends the use of centralized IAM solutions, especially for globally active companies.
- Data misuse, ransom payments, and fines for non-compliance are significantly reduced.
- The company can manage all authorizations centrally, keeping a close eye on the access rights of all employees, partners, and devices.

2 Bundesamt für Sicherheit in der Informationstechnik, ORP-Organisation und Personal, ORP-4: Identitäts- und Berechtigungsmanagement, Februar 2020

5. Defining key figures for an IAM business case

The definition of key performance indicators is essential for the implementation and control of an IAM system. A distinction must be made between key performance indicators (KPIs) and key risk indicators (KRIs). The monetary evaluation of an IAM program with economically oriented KPIs is much more difficult than using KRIs for the business case. Decision-makers primarily look at economic KPIs to allocate budget for an IAM investment. In the case of IAM, such a consideration comes up short, as the topic of security takes up a large share. Therefore, it is recommended to include KRIs in the business case. The monetary evaluation of such metrics can include potential ransom payments, or the loss of sensitive company data such as innovations and blueprints if privileged employees leave the company and move to the competition. In addition, penalties for non-compliance with regulatory requirements are part of the monetary valuation.

5.1. Key Performance Indicators (KPIs)

If an ROI calculation is used to justify an IAM program, pitfalls can lurk:

Pitfall number 1: ROI within IT
Don't try to calculate ROI within IT alone. A modern IAM program has an impact on a large number of business units. If you only consider the reduced administration costs for IT, the IAM investment hardly pays off. However, if you add up the benefits of all business units, the ROI increases accordingly.

Pitfall number 2: ROI over business
SSO and automated password reset increase productivity in the company. In addition, identity lifecycle management and role management make identities "workable" more quickly. However, the costs often have to be borne by the IT budget, as there are usually no cross-departmental budgets available in the company. The operational business is often not willing to contribute to the financing because of the perceived lack of benefit. Exception: Customer Identity and Access Management (CIAM) can have a quantifiable economic benefit.

The formulation of the following success indicators helps to demonstrate the success of an IAM program. The figures have been collected during the implementation of various IAM projects in companies:

- Reduction of annual operating costs in the area of desktop service and operation of applications by 44%
- Halving the number of employees and the associated personnel costs in the area of users, software and asset management through strong automation of the manual processes

- Achievement of a payback period of only 1 year for the project with an investment of € 1.7 million.
- Increased transparency through the possibility of allocating HW/SW costs to the originator (cost center-specific)
- Change in ordering behavior of employees through cost transparency: reduction of SW costs per user by 50 percent and reduction of PCB inventory by more than 20 percent
- Increased user satisfaction through self-service applications
- for staff and faster and error-free administration and provisioning processes for authorizations, moves, SW/HW packages, etc.
- Achieving conformity with the requirements of the Works Constitution Act (insight into SW and access rights per employee)

Often, other benefits are used to describe the success of a project. However, the following aspects are difficult to quantify:

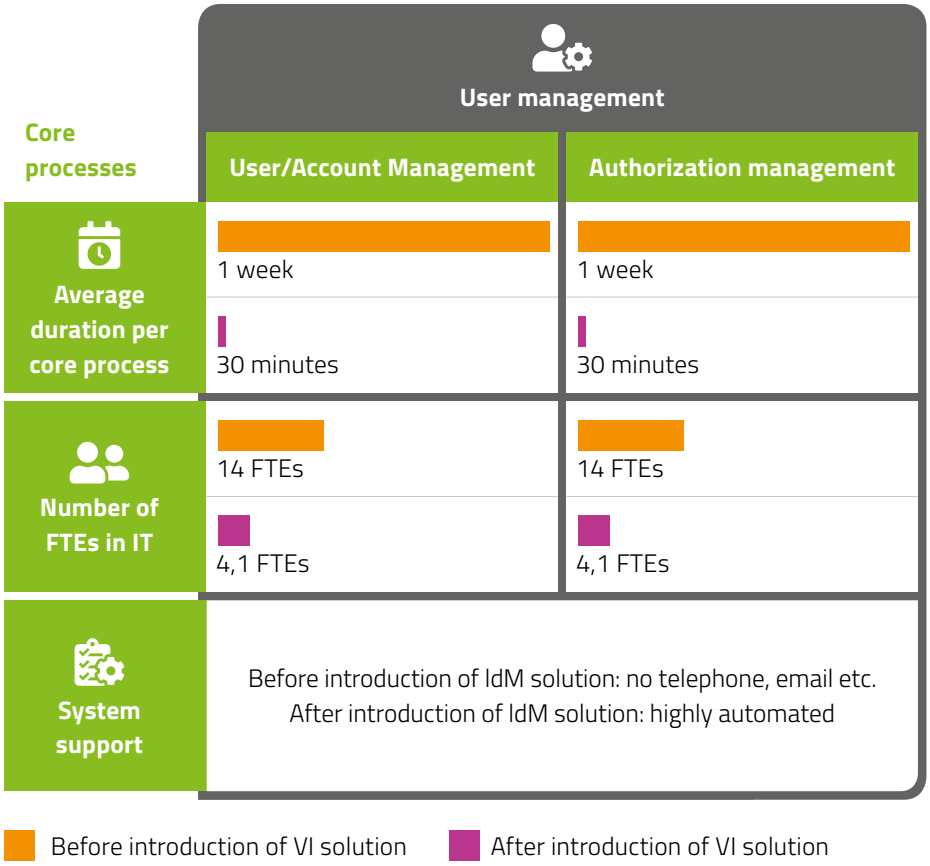
- User satisfaction: important argument and quantifiable, but how do you calculate the business "value"?
- Risk-driven investment: Often difficult to quantify and not at all monetarily assessable
- Compliance-driven investment: Organizational "solutions" are often sought in such cases. They are only quantifiable in regulated industries, but then they are often "binary".
- Business enablement through higher efficiency of provision: Monetary calculation is complex and offsetting practically non-existent.

Further examples of KPIs in the dimensions of efficiency, effectiveness, and enablement

Efficiency	Effectiveness	Enablement
▪ Turnaround times of orders ▪ Number of helpdesk calls ▪ Ratio of direct assignments versus rule or role-based assignments	▪ Coverage rate of managed versus administered applications or authorizations ▪ Reduction of administrative effort through roles ▪ Overcoming or avoiding audit findings	▪ Easier onboarding of business partners ▪ User satisfaction ▪ Support for new business models

Another approach is to focus on **reducing process time and saving massive amounts of resources through automation.** The following graphic shows a sample calculation

Figure 4:
Economic analysis for the introduction of an identity management (IdM) solution focusing on automating the employee life cycle (own presentation from a customer project, 2019)



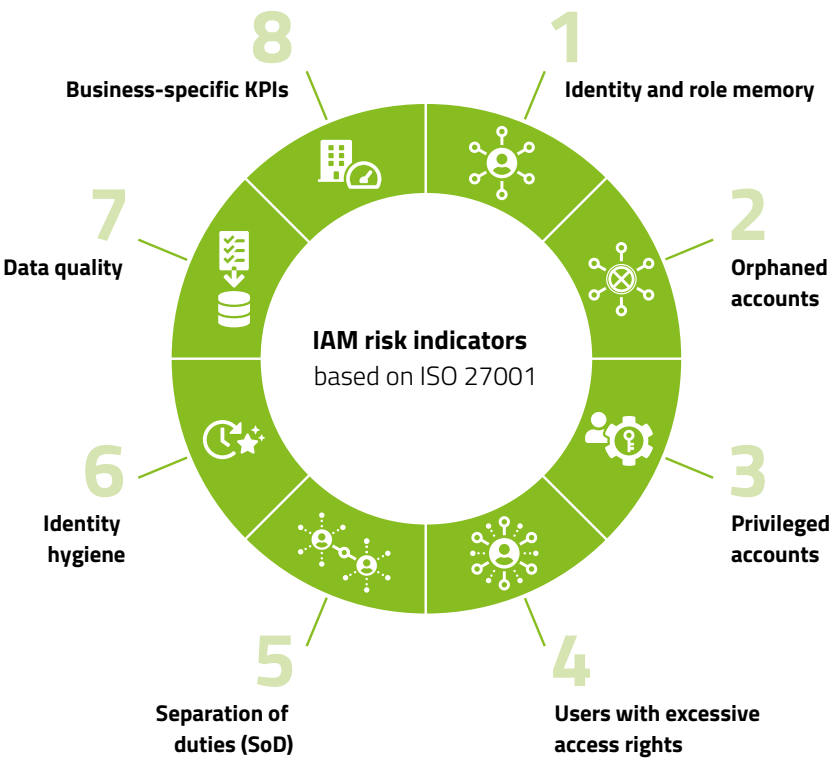
5.2. Key Risk Indicators (KRIs) according to ISO 27001

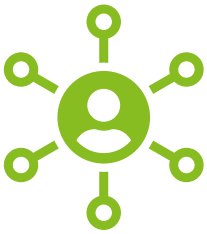
Based on ISO 27001 – the industry standard for information security – 8 different groups of KRIs are given, which can be used to present a business case. The following rules of thumb and analysis metrics are based on experience gained during the implementation of various IAM customer projects.

The risks range from data loss and misuse of confidential information, to downtime and business interruption.

IMPORTANT: If your team is unable to quantify most of the metrics due to insufficient data, then you have a strong case for purchasing an IAM system.

Figure 5:
IAM risk indicators based on ISO 27001





1. Identity and role memory

Even relatively simple metrics about the size of the identity and role memory provide an initial assessment of the quality of the IAM processes. If the number of users in the IAM system far exceeds the number of employees (often found in an HR system), something is probably wrong. Furthermore, observing the evolution of these metrics over time can reveal interesting trends (e.g. growth rates). For example, consider an almost constant increase in the number of roles. Furthermore, the value of metrics should not be underestimated as they give a good indication of the manageability of the IAM system.

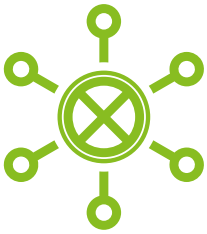
Examples:

- The number of applications integrated in the current IAM system
- The number of roles in relation to the number of departments
- The number of IT roles in relation to the number of business roles
- The number of authorizations in relation to the number of users
- The number of authorizations in relation to the number of roles

Rule of thumb:

What is the ratio between the number of roles and the number of users in your organization?

The total number of roles should not exceed 10 per cent of the total number of users. In many organizations that do not have adequate role management, this percentage is much higher. This means an overly complex role model that is difficult to maintain and can lead to errors and operational inefficiencies.



2. Orphaned accounts

One way to gain access to company resources, applications, or systems is through accounts that are no longer actively used. This applies to accounts of employees who have left the company, as well as external contractors who have completed a project in the company. Companies that do not take the necessary steps to close these access points leave the door open to attackers.

When a user's employment ends or a contractor's project is finished, their user accounts must be deactivated (i.e. turned off). This should be part of the offboarding process (often automated by the IAM system) for employees and contractors. In practice, however, these accounts may be deactivated incorrectly – or not at all. Identifying and cleaning up these accounts significantly reduces the risks. By finding out why these accounts have not been deactivated, IAM processes (offboarding) can be improved.

Some metrics on orphaned accounts:

- Users who have not logged in for some time, or accounts that have not been used for a certain period of time, are also known as dormant accounts. Exactly how long this period should be can vary from company to company. However, 90 days is often considered the threshold. For certain accounts, such as administrator accounts, a shorter period may make sense compared to other accounts. Therefore, this KPI can be split into several sub-KPIs.
- Users who have never logged in.
- Uncorrelated user accounts, also known as ghost accounts. These are accounts that are not linked to an active user or any user at all.
- User accounts with a status that indicates inactivity. Exactly what this status depends on the IAM system used in the organization, e.g. "retired" or "inactive". The clue is to look at the user properties in the IAM system that might indicate that an account is not in use.

3. Privileged accounts

Privileged accounts, those that have significantly more access rights than normal accounts, come in many shapes and forms. However, if not properly managed and monitored, privileged accounts pose significant security risks. These risks can come from all sides: from malicious "outsiders" (e.g. hackers) or from careless or disgruntled "insiders". Whoever gains access to these privileged accounts can control company resources, access sensitive data, or even change or deactivate (security) systems.

It is important to know how many and what type of privileged accounts exist in the organization. Note, however, that some of the types of privileged accounts mentioned below may overlap:

- Administrator accounts, such as Local Admin or Domain Admin.
- Hidden accounts. These have administrative rights on one or more systems, but often exist under the radar because they are not marked "Admin".
- Privileged service accounts such as domain service accounts.
- Non-Personal Accounts (NPA). These accounts are not directly related to a clearly identifiable person/employee and they are not the result of the Joiner/Mover/Leaver HR processes in an organization. Such accounts are often quite powerful (e.g. admin or root account) but difficult to identify. In addition, logging in with the account leaves no audit trail showing which person actually used it. In other words, there is no specific person who can be held accountable.
- Privileged role-based accounts. Depending on the role model, certain roles can be considered privileged. Therefore, we should consider users who are assigned one or more of these roles as privileged accounts.

- Privileged data user accounts. Even though these users are not typical privileged accounts, they should still be considered privileged because of the sensitive data they can access. Think of the accountant who has access to their clients' financial data, a human resources employee who has access to sensitive employee data, or a doctor who has access to patient data.

4. Users with excessive access rights

The difference between privileged accounts and users with excessive access rights is that the former focus on users who by definition should have (many) sensitive access rights, while the latter focus on users who inadvertently have (too) many access rights. One of the most important principles of information security is the Principle of Least Privilege (PoLP). This principle states that users' access rights are limited to the absolute minimum they need to perform their intended work. It is a common misconception to think only of malicious employees when applying PoLP. Rather, employees can also inadvertently disclose data through phishing or a lost laptop. But whether intentional or not, the less data your employees can lose, the better.

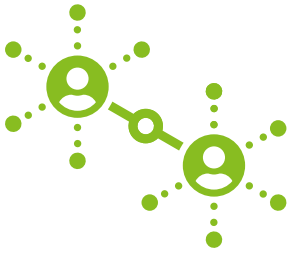
It is a fact that the cumulative access rights and permissions of all users together determine the size of your organization's attack surface, which should of course be kept as small as possible. Unfortunately, there is often a gap between the access rights granted and those actually used. This indicates that users have too many access rights, which unnecessarily increases your attack surface.

- Outliers: These are users who have more access rights (i.e. who have been assigned more roles or have more privileges) than their colleagues. Often this is the result of a change in department or function of staff without the previous – and now unnecessary – access rights being revoked. Another way to find outliers is to compare them to an ideal role profile. Depending on the function a particular employee holds, a certain set of roles may be appropriate. However, this only applies to organizations that work with such role profiles.

- Users who have been assigned a large number of roles or permissions. What is considered "high" depends on the role model and the organizational context.

Rule of thumb:

A rule of thumb for when a user can be identified as having a high number of roles or permissions is when the total number of roles or permissions exceeds twice the average.



5. Separation of duties (SoD)

Separation of duties or functions, also known as segregation of duties, is considered one of the most difficult and often costly identity controls to implement properly. The aim is to distribute tasks and the associated permissions among several people. In this way, it is much more difficult to commit fraud, as it requires at least two people to work together. However, the goal is no longer limited to fraud prevention, but also includes security and data protection. When SoD is properly designed and implemented, it ensures that employees do not have conflicting responsibilities or interests. For example, the person who sets a policy should not have the ability to approve its execution. Apart from the SoD controls themselves, metrics are important to see how you are progressing:

- SoD violations. In addition to the total number of SoD violations, it may also be interesting to look at the number of specific SoD violations. This is to identify "toxic" combinations that appear to be the most difficult to circumvent. For these violations, tactical clean-up is unlikely to be sufficient. However, a strategic redesign could improve the situation.

- Unclear combinations of access rights. These are combinations of roles, permissions or applications where it is not clear whether they are considered "toxic" or not. When such a combination occurs in practice, it is important to know whether it is allowed or not in order to take appropriate action (if necessary).

How is the implementation of an SoD control approach started?
The implementation of an appropriate SoD control set starts with the definition of "toxic" combinations of access rights (roles, permissions, applications, etc.). If users have such combinations of access rights, this should be mitigated or remedied. However, manual control of SoD violations is very time-consuming and error-prone. Therefore, the key to risk mitigation is automation, i.e. to identify SoD conflicts using an agile approach.

6. Identity hygiene
It is important to recognize that identity hygiene (i.e. proper maintenance of the memory) and information security are closely linked: A well-maintained IT environment is better protected against information security risks. Applying best practices for users, roles, and permissions not only helps prevent risks, but is also much easier and requires much less effort than a situation where you have to clean up regularly. In other words, prevention is better than cure.

Some metrics to measure your level of user hygiene:
- Users who are not assigned any roles or permissions.
- Users who do not have access to any applications.
- User accounts that have not been changed for a certain period of time. Exactly how long this period should be can vary from company to company.
- User accounts with direct permissions that are not assigned via roles.
- User accounts for testing purposes (i.e. test accounts).
- Users (and in particular their access rights) who have not been checked for a certain period of time. Again, the exact time period may vary from can vary from company to company and often depends on the frequency of recertification campaigns. This KPI can also be set up for specific types of accounts, such as administrator accounts.
- If the organization enforces a password expiry policy: User accounts with expired passwords.

7. Data quality
In order to obtain accurate results from all of the above controls, it is crucial that all relevant data ("attribute values") are entered correctly. The KPIs only reflect the actual state if the data in the IAM system is correct, complete and up-to-date. Many of the processes such as onboarding, offboarding and more generally changing data are automated with the help of IAM systems. Finding inaccuracies or empty fields is therefore also an opportunity to improve these processes. Specific data problems cannot be solved without addressing the root cause.

There are many KPIs that help measure this. Think of all the different data attributes in the IAM system that could be left blank. However, it is important to focus on the attributes that are critical to other KPIs or to take action to improve identified problems. Remember that deeper information and actionable insights are needed to actually improve identified problems. Without the right information, it is almost impossible to decide whether or not a particular user account or role can be disabled/suspended.

Some metrics that are essential for most companies:

- Users without manager, department, and email.
- Roles without (correct and clear) description and owner.
- Permissions without (correct and unambiguous) description and owner.
- Applications without (correct and unambiguous) description and owner.

8. Business-specific KPIs

In addition to the more general KPIs mentioned in the previous sections, it is important to complement these KPI sets with business-specific metrics. In financial institutions, for example, it is often the case that an employee needs appropriate certification/ training to perform a certain activity. One such business-specific KPI could therefore be the number of employees who are authorized to perform that action but do not have the relevant certification. Another common situation is that companies focus on security awareness training and want to measure for whom this training has taken too long, especially if these users have many permissions.

6. Summary

In conclusion, the business and risk drivers described above, and the identification of various KPIs and KRIs, provide initial arguments for initiating a change project for IAM at management and operational levels.

The development of an IAM business case often involves the involvement of various stakeholders from infrastructure, service, security, and HR. It is a multi-stage process consisting of vision, roadmap, architecture and business case. The communication of an IAM business case to the board and other decision-makers should not only be business-oriented, but also include risk-oriented metrics. Building a successful IAM program involves consensus among stakeholders, definition of business drivers, risk analysis, and definition of success metrics.

Reference (German language only): BSI ORP.4 – Identitäts- und Berechtigungsmanagement
https://bit.ly/3oOnDPc

About iC Consult

iC Consult is the world's leading independent consultancy, systems integrator, and managed services provider for Identity & Access Management with more than 800 employees worldwide.

We are committed to excellence and innovation, and with the best-in-class technology in the IAM space, we provide our customers with next-level cybersecurity solutions. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations.

iC Consult is headquartered in Germany with offices in Switzerland, Austria, France, Belgium, Spain, Bulgaria, the UK, the U.S., Canada, India, and China. The world's largest brands trust in our expertise, to secure and manage their most valuable assets: their identities.

More information at www.ic-consult.com