TOOLS4EVER

Whitepaper V1.0 / 25 08 2022

ISO 27001

and the role of Identity Management

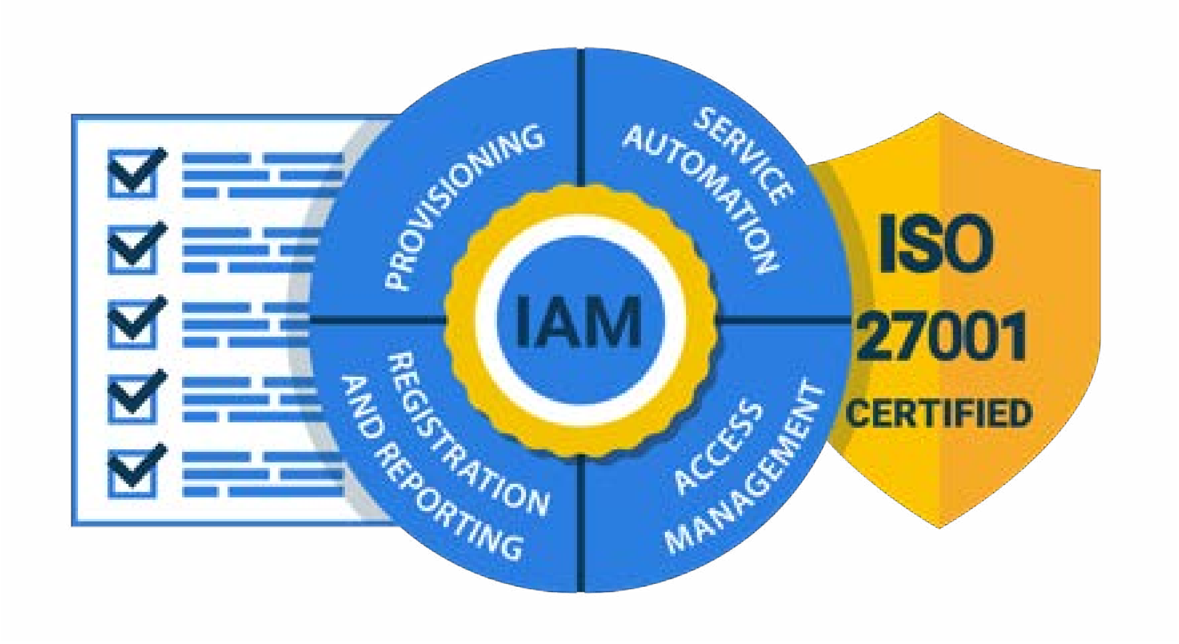
Table of contents

Introduction

ISO 27001 is the ultimate international standard for information security management. The standard assists organisations in securing their information systems with an Information Security Management System (ISMS) in a structured, effective and efficient manner. ISO 27001 is widely applied and also forms the basis for security standards within specific sectors, such as the Baseline Information Security Government (BIO) and the NEN 7510 (in healthcare).

ISO 27001 helps organisations in two ways. Firstly, it provides concrete guidelines for properly setting up and managing information security within the organisation. Additionally, ISO 27001 certification provides organisations with a generally accepted seal of quality. To customers and partners, it confirms that as an organisation, you have fully organised your information security and comply with the prevailing requirements. For collaboration agreements and contracts, an ISO 27001 certificate often constitutes a necessary 'tick the box' requirement.

In this whitepaper, we first provide an overview of the ISO 27001 standard. Then we explain the key role Identity Management plays in making your organisation ISO 27001 compliant.



ISO 27001 overview

SO 27001 does not contain detailed technical requirements for matters such as multi-factor authentication or data encryption. The standard focuses on information security management systems and is primarily intended to structure your organisation and processes in such a way that the confidentiality, availability and integrity of information is assured. ISO 27001 aligns with the so-called ISO High-Level Structure (HLS). This HLS provides a basic structure for management systems, with general guidelines in areas such as leadership, risk management and process management. Specific standards such as ISO 9001 (quality), ISO 14001 (environment) and ISO 27001 (information security) can be thought of as 'clicking' into the overall management system, thus creating a single coherent management system for your organisation.

ISO 27001 comprises 10 chapters and an annex. The substantive requirements are described in chapters 4 through 10 and are summarised below. In Annex A to ISO 27001, you will find concrete control objectives and measures that you must use – if they are relevant within your organisation – to actually implement information security. We will elaborate on this annex later on in this whitepaper.

Chapter 4-5: Business context

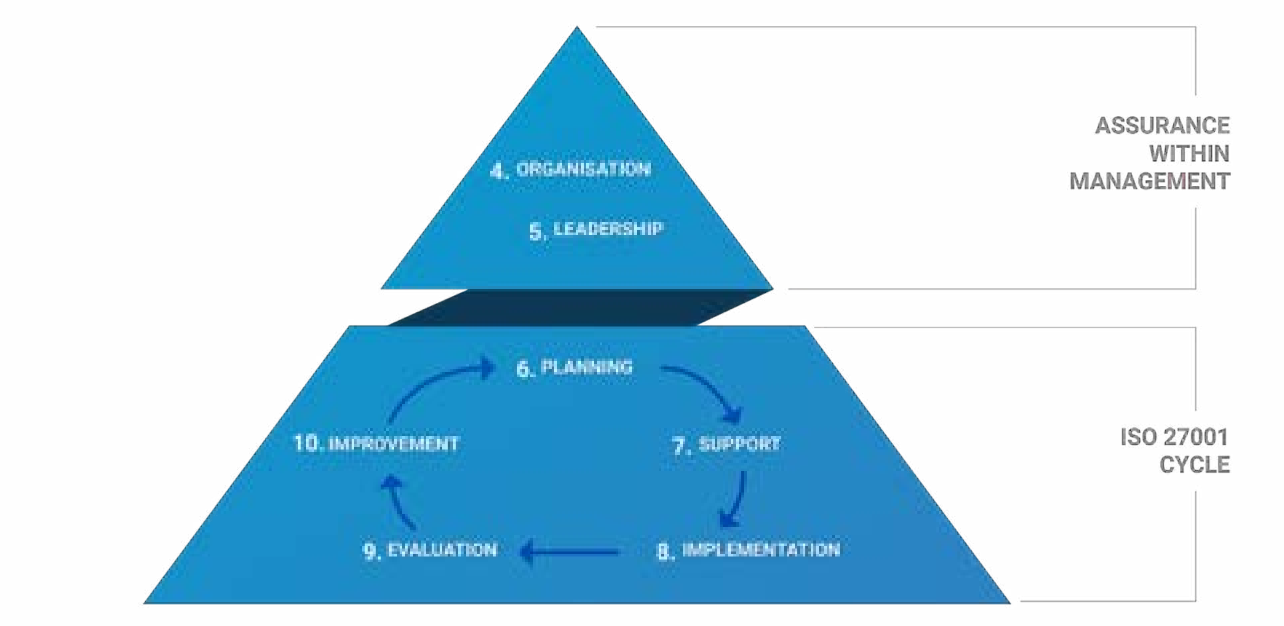
For ISO 27001, it is important that information security is positioned at a sufficiently 'high' level within the organisation. It is not enough to simply have 'a security plan' developed and managed by the IT department. Information security must align with the business objectives and operations, and security should be a matter in the hands of the top level of management. The first two chapters (4 and 5) describe these requirements.

4. ORGANISATION
5. LEADERSHIP
ASSURANCE
WITHIN
MANAGEMENT

H4. Context of the organisation	This is where we inventory the organisational context for information security. For instance, an academic hospital clearly has different security requirements than a car dealership. Therefore, it is important to inventory what objectives the organisation has, which internal and external stakeholders exist, what regulations apply, etc. Based on this information, you then determine the framework for the final information security plan.
H5. Leadership	Leadership is an important element. It is no coincidence that senior managers are interviewed during ISO audits. Information security should be the responsibility of that senior management and should not be delegated to a 'powerless' quality manager in a secondary building. Furthermore, the various roles and responsibilities for information security must be clearly defined.

Chapter 6-10: ISO 27001 'cycle'

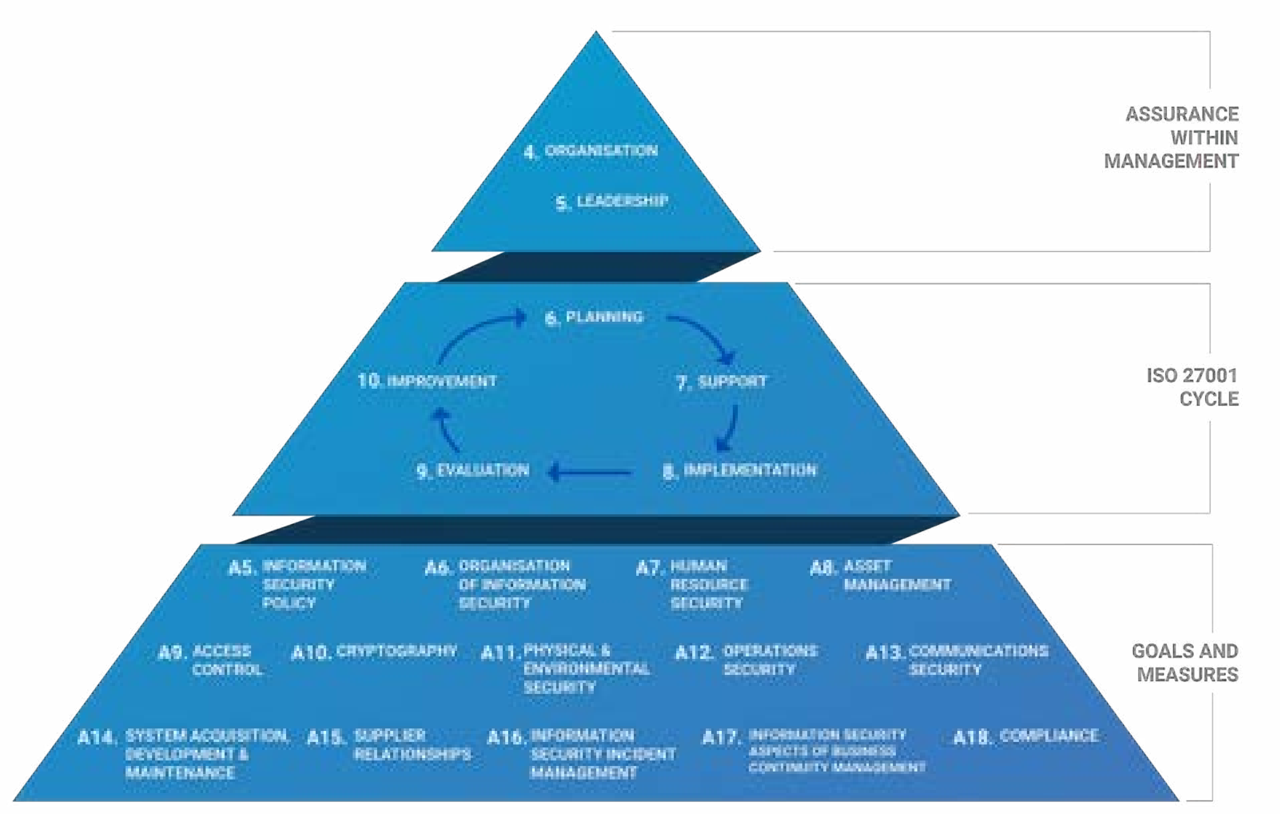
Chapters 4 and 5 ensure that the organisational frameworks are clear and that senior management is sufficiently involved. In the next few chapters, 6 through 10, you then find concrete guidelines on how to organise, plan, implement and continually adjust information security to the current circumstances:



H6. Planning	The foundation consists of a comprehensive risk analysis, taking into account the risks that are applicable to this organisation. For each risk, the likelihood of that risk is determined as well as its potential impact. Based on this, you establish the necessary measures to control the risks. You establish concrete security objectives and how you intend to achieve those objectives.
H7. Support	The organisation must, of course, be capable of executing these plans. The proper skills, knowledge, systems and 'security awareness' must be present. There must also be sufficient investments in internal communication and documentation.
H8. Implementation	The security processes must be implemented, accompanied by appropriate measures to manage safety risks. Throughout the implementation of the plans, results must be continuously monitored, and risk analyses must be regularly updated.
H9. Evaluation	The results of the security measures must be systematically evaluated. This includes internal audits and regular management reviews that should be prepared and discussed within the management team.
H10. Improvement	Finally, it must be ensured that not only are any deficiencies identified in the evaluations addressed, but also that the processes and competencies are in place to continually develop and implement new and improved security measures.

Annex A: Control objectives and measures

An organisation must meet all the requirements in the chapters of ISO 27001 in order to obtain certification. How these requirements are met may depend on the type of organisation and its objectives. In Annex A to ISO 27001, you will find an overview of 114 different control objectives and measures, divided into 14 categories. You can look at this annex as a catalogue from which each organisation must deploy measures that are applicable to their own organisation and risks. There is also the standard ISO 27002, which further elaborates on the various measures. Below you will find a brief overview of the categories with the objectives and measures in Annex A.

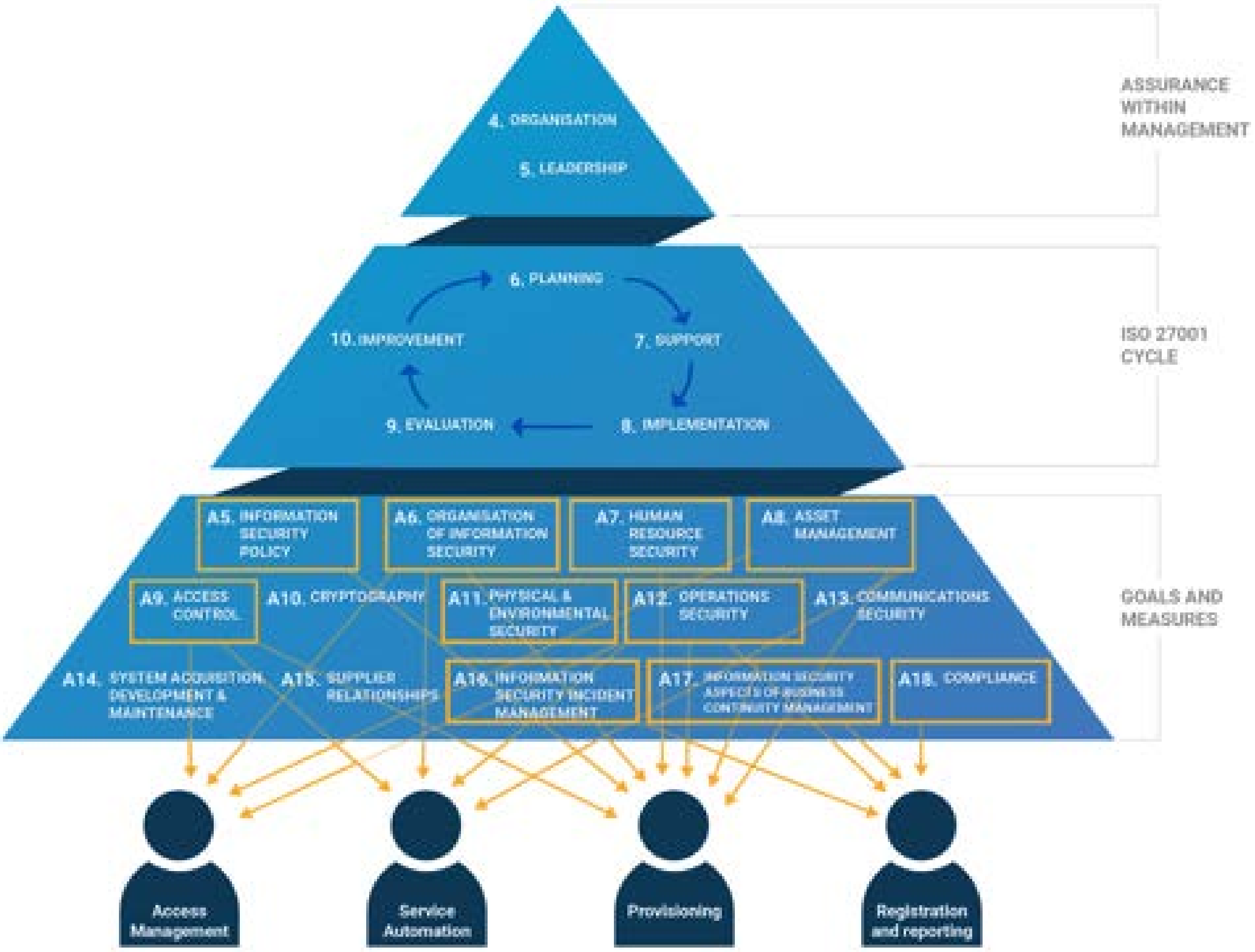

4. ORGANISATION
5. LEADERSHIP
ASSURANCE WITHIN MANAGEMENT
6. PLANNING
7. SUPPORT
8. IMPLEMENTATION
9. EVALUATION
10. IMPROVEMENT
ISO 27001 CYCLE
A5. INFORMATION SECURITY POLICY
A6. ORGANISATION OF INFORMATION SECURITY
A7. HUMAN RESOURCE SECURITY
A8. ASSET MANAGEMENT
A9. ACCESS CONTROL
A10. CRYPTOGRAPHY
A11. PHYSICAL & ENVIRONMENTAL SECURITY
A12. OPERATIONS SECURITY
A13. COMMUNICATIONS SECURITY
A14. SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE
A15. SUPPLIER RELATIONSHIPS
A16. INFORMATION SECURITY INCIDENT MANAGEMENT
A17. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
A18. COMPLIANCE
GOALS AND MEASURES

A5. Information security policy	In addition to the general organisational policy, a specific information security policy must also be established and regularly evaluated.
A6. Organisation of information security	It is not enough to simply have an information security policy in place; it also needs to be implemented and managed. What roles are needed in combination with which responsibilities and authorities? Role separation is an important focus, and nowadays there is also a great need for attention to online working and the use of (personal) mobile devices.
A7. Human resource security	Employees must be adequately trained and aware of the importance of information security. This applies throughout the entire 'employment lifecycle', from proper recruitment of employees to ensuring the necessary security measures when people leave the organisation.

A8. Asset management	Assets that process information (such as software and computer systems) must be well recorded and well managed. Who is allowed to use the systems, and are assets and usage rights returned and withdrawn after work activities end? All information must be properly classified and stored securely.
A9. Access control	Measures are needed to ensure that employees have access only to networks, systems and data they need for their own work.
A10. Cryptography	Data must be sufficiently encrypted to guarantee both the confidentiality and integrity of the information.
A11. Physical and environmental security	Organisations must prevent unauthorised access to computers and information carriers at office locations. This also means that in the event of power failures or emergencies, for example, information security must remain intact. And upon disposal of equipment, data must be erased.
A12. Operations security	Clear agreements and procedures must be in place to ensure the safe use of information systems and to protect the systems against malware. Clear backup and monitoring measures are also needed.
A13. Communications security	Both internal network facilities and external network communication must be secured against unauthorised access and misuse.
A14. System acquisition, development and maintenance	Organisations must consider the security of systems and data when purchasing, developing and managing IT systems. This not only includes operational systems but development, demo and test systems must also be adequately secured.
A15. Supplier relationships	Organisations depend on suppliers for their IT systems. This applies to on-premises systems and software, as well as suppliers that manage sensitive cloud-based data. Clear agreements with suppliers are needed in order to ensure information security.
A16. Information security aspects of business continuity management	Despite all security measures, an incident can still occur. Hence, proper procedures with clear responsibilities are required ahead of time to deal with such an incident. This includes putting in place agreements on further reporting and resolution.
A17. Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	In the event of IT related incidents, specific care must be taken to make sure that the continuity of information security is always guaranteed.
A18. Compliance	As an organisation, you must continually be able to demonstrate that you comply with all applicable laws and regulations.

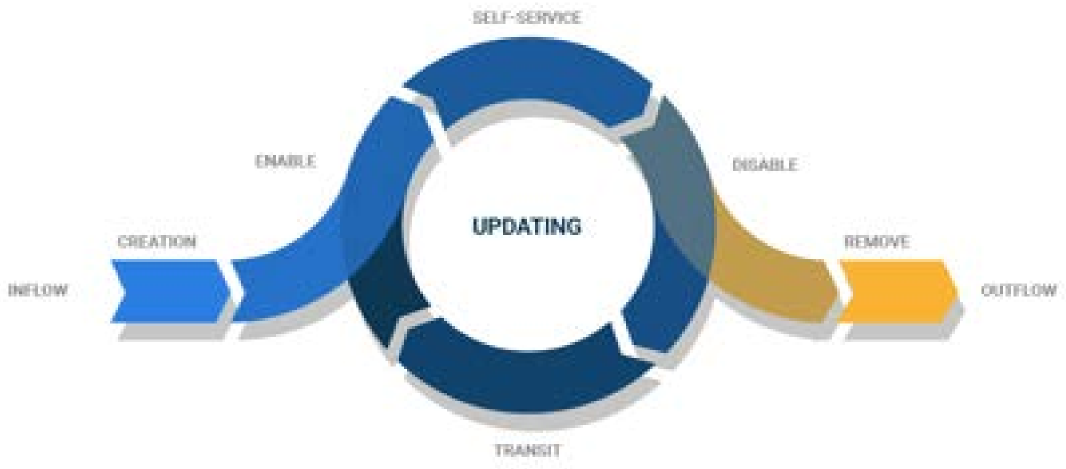
Identity Management and ISO 27001

As we mentioned, Annex A to ISO 27001 provides a more detailed view of the measures an organisation must take to properly secure information. In this context, the management of end-users and their rights is becoming increasingly important. Employees, partners and customers should only have access to applications and data on a 'need to know' basis. It is also essential that all IT activities can be traced down to the level of individual users. This makes Identity Management an important tool in the realisation of 'ISO 27001 proof' information security. In this chapter, we map the various categories of measures in Annex A to the capabilities of a state-of-the-art Identity Management solution. We illustrate this using our own HelloID cloud-based Identity & Access Management (IAM) platform.


4. ORGANISATION
5. LEADERSHIP
ASSURANCE WITHIN MANAGEMENT
6. PLANNING
7. SUPPORT
8. IMPLEMENTATION
9. EVALUATION
10. IMPROVEMENT
ISO 27001 CYCLE
A5. INFORMATION SECURITY POLICY
A6. ORGANISATION OF INFORMATION SECURITY
A7. HUMAN RESOURCE SECURITY
A8. ASSET MANAGEMENT
A9. ACCESS CONTROL
A10. CRYPTOGRAPHY
A11. PHYSICAL & ENVIRONMENTAL SECURITY
A12. OPERATIONS SECURITY
A13. COMMUNICATIONS SECURITY
A14. SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE
A15. SUPPLIER RELATIONSHIPS
A16. INFORMATION SECURITY INCIDENT MANAGEMENT
A17. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
A18. COMPLIANCE
GOALS AND MEASURES
Access Management
Service Automation
Provisioning
Registration and reporting

Provisioning of user accounts and rights

Group accounts are not acceptable under ISO 27001, just as the 'copy user' principle for newly incoming employees is also not acceptable. Nowadays, access rights must be unambiguously linked to individual user accounts. It must be clear at all times who has access to what data and applications, and who performs certain actions. And of course, account information and access rights must always be up to date. This means they must always be in line with someone's current role and position within the organisation. Professional and automated user account management is crucial in achieving this goal.



Within HelloID, we ensure this through automated provisioning. This keeps a person's digital identity and access rights aligned with the information registered in the HR system at all times. Thanks to a direct link between the HR system and HelloID, the new employee receives a user account immediately upon onboarding, with facilities and rights attached that are appropriate to their role. We also keep this automatically updated throughout their employment. If someone's role changes, HelloID immediately adjusts the access rights accordingly. And if someone leaves the organisation, HelloID ensures that the account is automatically blocked, and the departing employee no longer has access. Accumulation of rights and accounts that inadvertently remain accessible is no longer possible.

Service Automation: standardisation with room for exceptions

Effective information security relies on clear policy guidelines, transparent processes and limited scope for individual and uncontrolled customisation. To ensure this, we aim to standardise and automate identity management processes to the greatest extent possible. This should enable us to support concepts such as role-based access and implement processes with a clear separation of roles. At the same time, there will always be exceptions, and each organisation must find its own balance between user-friendliness and business security. Automatically granting excessive permissions leads to unwanted security risks. However, unnecessarily delaying employees in obtaining their access rights hinders their work.

HelloID offers the desired combination of standardisation and exceptions:

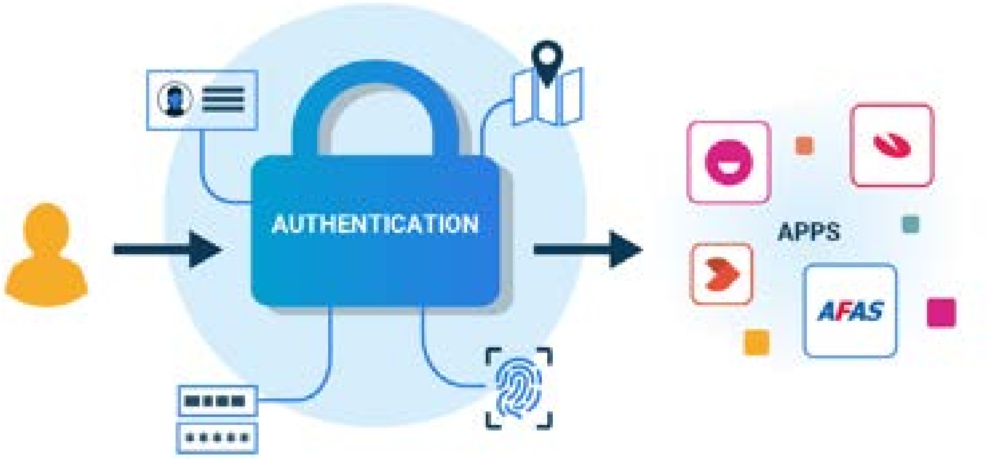
- Within HelloID, you can assign permissions using the Attribute Based Access Control (ABAC) feature as standard. We translate the organisational structure with roles and associated tasks into configurable business rules within HelloID, which then automatically determines access rights for an employee. This automation covers everything from automatic onboarding upon joining to the departure procedure upon leaving the organisation.

- The majority of permissions are therefore fully automated, but such a standard role-based matrix is never entirely comprehensive. That is why HelloID also provides for exceptions. For more specific and difficult-to-automate permissions, you can design self-service processes. Users can request online access to applications or data shares themselves, while ensuring that the appropriate approval steps are automatically followed. Following approval, the automated process ensures further activation without risky exceptions or mistakes.

Automated configuration rules ensure that the service catalogue automatically remains up to date. For instance, a new share becomes immediately visible in the catalogue. At any given time, the system can provide an overview of which employees are active and which licenses, applications, shares, etc., they are using.

Access management

State-of-the-art access management ensures that employees - and, when necessary, partners and customers - can easily and consistently access applications and data. As explained earlier, the principle here is that each user is equipped with a single personal user account. Through a concept such as Single Sign-On (SSO), you ensure that people only need to log in once. Such a combination of user-friendly and secure access solutions prevents employees from devising unsafe workarounds.



HelloID supports all common Single Sign-On protocols to authenticate users for each application. For access to applications without built-in SSO capabilities, HelloID provides alternative methods to facilitate access. For primary authentication, we can integrate HelloID with Active Directory and other so-called Identity Providers such as Azure, Google, Salesforce, SAML and OpenID. The platform also supports additional security options such as Two-Factor Authentication (2FA). HelloID recognises contextual factors such as login location and time, and can prompt the user for additional authentication based on those factors. In addition to soft or hard tokens and SMS, HelloID also offers various one-time passwords (OTPs) as a second factor.

HelloID provides Identity & Access Management from the cloud, offering the advantages of lower investments, rapid installation and configuration, while Tools4ever handles the technical management, including automatic updates. The solution is implemented using highly secure Microsoft Azure and Google Cloud environments, which are rigorously audited by Deloitte Risk Services every six months. Compliance with stringent security requirements is thus assured. Furthermore, the service has very high availability due to built-in redundancy.

Reporting

Registration and reporting are essential to ISO 27001 compliance. As an organisation, you must be able to demonstrate that various processes are carried out in accordance with relevant laws and regulations. Additionally, in the event of a security incident such as a data breach, you must be able to trace which users within the network performed what actions.

As a cloud-based solution, HelloID must adhere to increasingly stringent regulations regarding audits and security. Therefore, all access attempts, automated and manual processes and the use of our platform are recorded in a way that makes them easy to screen. This means that the authentication process is automatically monitored, and through reports, it is always clear who accessed which applications, at what point in time, and from which location. This not only provides a detailed view of the authentication journey, but also reveals login attempts from suspicious IP addresses, for example. Potential threats can be identified in a timely manner, allowing for the deployment of countermeasures.

What sets HelloID apart is that within the system, the entire identity lifecycle is auditable, both per system and per user. All actions are logged, including creating, activating, updating, moving, disabling and deleting accounts. The same applies to granting and revoking permissions. If permissions are granted ad hoc (outside the regular role-based matrix), HelloID precisely shows who requested this, who approved the request and the exact changes it led to in the underlying systems. This makes the HelloID process fully transparent, auditable and adaptable.

Want to learn more?

Identity Management plays a central role in your IT security today. Employees, partners and customers should only have access to applications and data with their own accounts. Rights should always be granted on a 'need to know' basis. Moreover, we should be able to trace all IT activities down to the level of individual users. This makes your Identity Management platform an important element in setting up your ISO 27001-compliant information security system.

Interested in learning more about the role Identity Management can play in ISO 27001 compliance within your organisation? And how can you keep your IT environment secure without compromising on user-friendliness? We would be happy to provide you with more information, for example, using our ISO 27001 - HelloID checklist. In this list, we cover all ISO 27001 Annex A measures, with an explanation for each measure or, if applicable, details on how HelloID Identity Management can contribute to it.

TOOLS4EVER

Address	102-103 Church Street, GL20 5AB, Tewkesbury, UK
General	+44 (0)1684 274 845
Support	+44 (0)1684 270 822
Information	uksales@tools4ever.com
Sales	uksales@tools4ever.com
Support	uksupport@tools4ever.com