TOOLS4EVER

Whitepaper V1.0 / 25 08 2022

HelloID contribution to ISO 27001

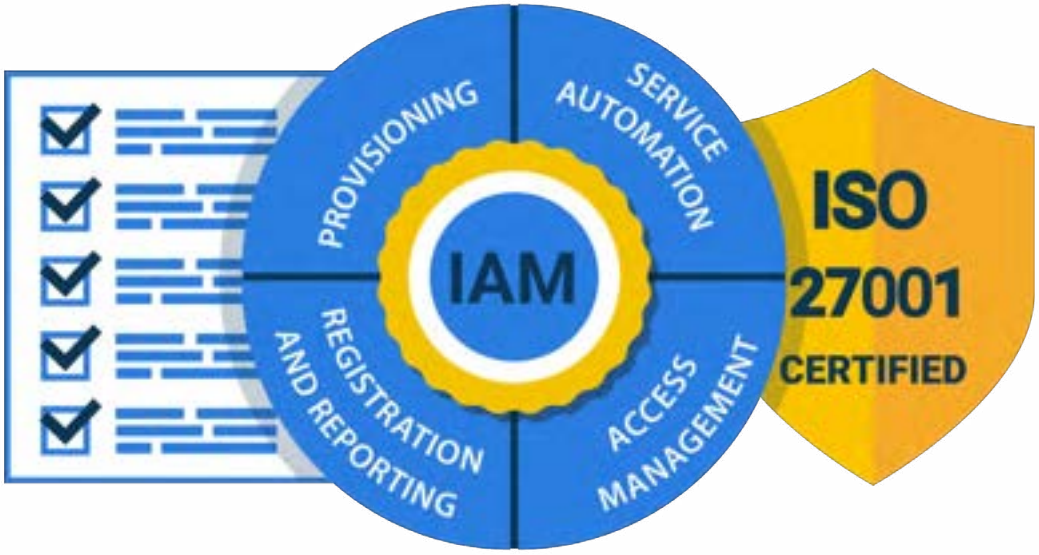
Inhoudsopgave

Introduction

This document describes how the HelloID Identity Management platform contributes to making customer organisations ISO 27001 compliant. It does not address whether the HelloID platform complies with specific guidelines in these standards. This document focuses on how HelloID supports organisations in achieving security objectives and the associated measures. For example, HelloID's role-based access control is a central element in the access security of all IT systems within a customer organisation. The fact that HelloID creates backups only means that HelloID itself meets the requirements. Tools4ever, as the developer of IDaaS solution HelloID, is fully ISO 27001 certified.

ISO 27001 helps organisations in two ways. Firstly, with concrete guidelines for properly setting up and managing information security within the organisation. In addition, organisations with an ISO 27001 certification benefit from a generally accepted quality mark. To customers and partners, this confirms that your organisation has its information security fully in order and meets the applicable requirements. For collaboration agreements and contracts, such an ISO 27001 certificate often constitutes a necessary 'tick the box' item.

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



ISO 27001 overview

ISO 27001 does not provide detailed technical requirements for topics 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 confidentiality, availability and integrity of information is guaranteed. 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 integrated into the overall management system, so that your organisation achieves a cohesive management system.

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 which – if they are relevant within your organisation – you must use to actually implement information security. This annex is further discussed later on in this whitepaper.

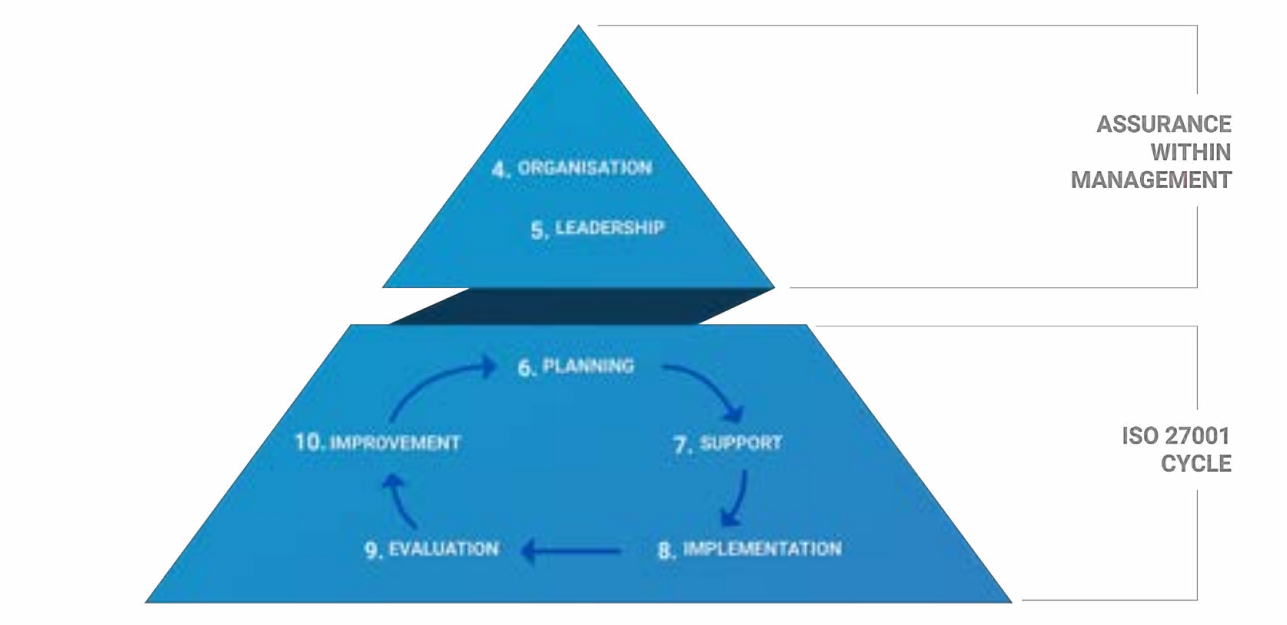
Chapters 4-5: Business context

As part of ISO 27001, it is important that information security is assigned a sufficiently high priority level within the organisation. It is not enough to simply have a 'security plan' drawn up and managed by the IT department. Information security must align with business objectives and operations, and security must be on the agenda at the highest level of management. The first two chapters (4 and 5) describe these requirements.

H4. Context of the organisation	This is where we inventory the organisational context for information security. For example, 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, which regulations apply, etc. This will determine the framework for the final information security plan.
H5. Leadership	Leadership is an important component. It is for good reason that senior managers are also interviewed during ISO audits. Information security should be the responsibility of that senior management and not delegated to a 'toothless' quality manager in some annex building. Moreover, the various roles and responsibilities in terms of information security must be clearly established.

Chapters 6-10: ISO 27001 'cycle'

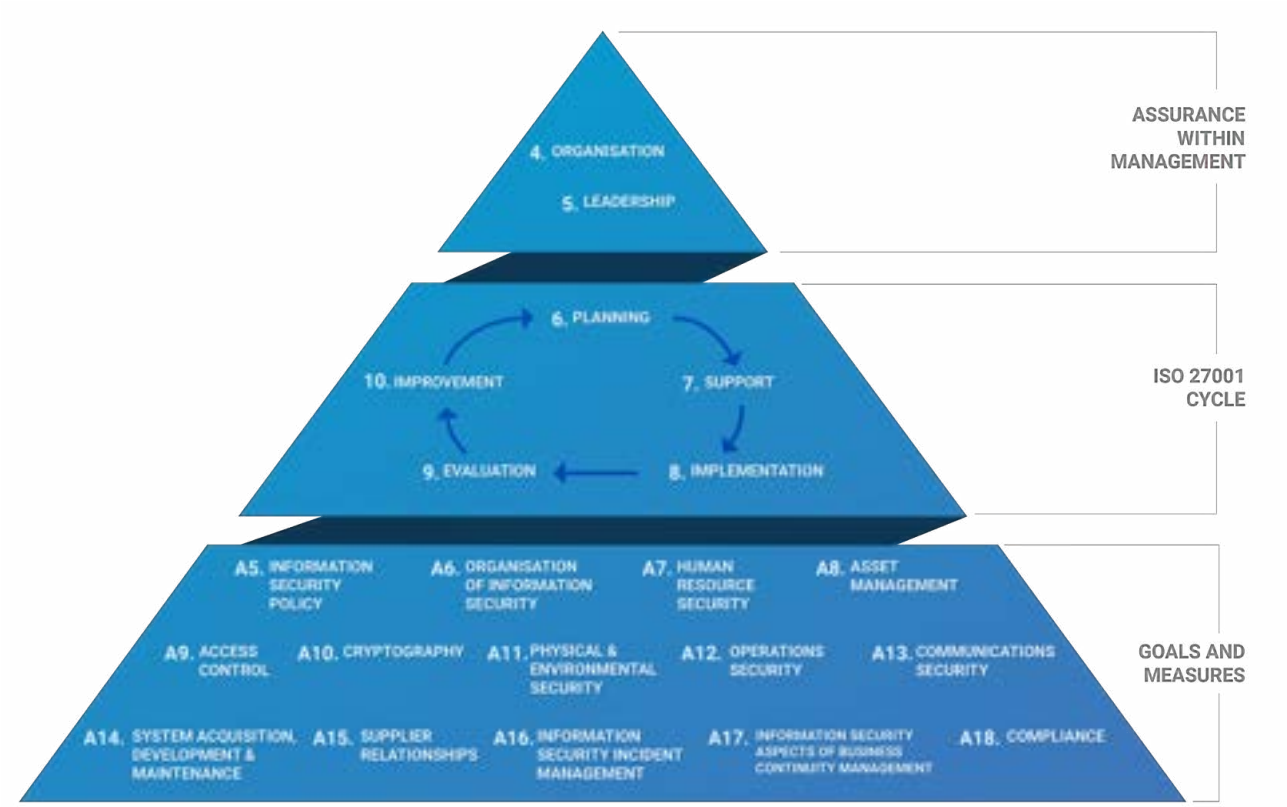
With chapters 4 and 5, you ensure that the organisational frameworks are clear and that senior management is sufficiently involved. In the following chapters 6-10, you then find guidelines on how to concretely organise, plan, implement and continually adjust information security to the current circumstances:



H6. Planning	The basis consists of a comprehensive risk analysis for the risks that are applicable to this organisation. For each risk, the likelihood of that risk and its potential impact are determined. Based on this, you establish the necessary measures to control the risks. You establish concrete security objectives and strategies for how you are going to achieve those objectives.
H7. Support	Naturally, the organisation must be capable of actually executing these plans. The correct skills, knowledge, systems and 'security awareness' must be present. Adequate investment in internal communication and documentation is also required.
H8. Operation	The security processes must be implemented with the appropriate measures to control the security risks. During the execution of the plans, the results must be continuously monitored and the risk analyses regularly updated.
H9. Evaluation	The results of the security measures must be systematically evaluated. This includes internal audits and also, a so-called management review should be regularly prepared and discussed within the management team.
H10. Improvement	Finally, it must be ensured that not only the potential shortcomings from those evaluations are resolved. The processes and competencies to constantly develop and implement new and improved security measures must also be present.

Annex A: Control objectives and measures

You must meet all the requirements in the chapters of ISO 27001 to become a certified organisation. The fulfilment of the requirements may depend on the type of organisation and objectives. In Annex A to ISO 27001, you will find an overview of 114 different control objectives and measures, split into 14 categories. This annex can be seen 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.



A5. Information security policy	As an addition to the general organisational policy, a specific information security policy must also be established and regularly evaluated.
A6. Organisation of information security	Not only is an information security policy needed, but it also needs to be implemented and managed. Which roles are necessary and what are their respective responsibilities and authorities? Role separation is an important point of consideration, and nowadays, there is also a significant need for attention to remote working and the use of (personal) mobile devices.
A.6.1.2 Segregation of duties	With HelloID, organisations can configure approval processes for the various (self-)service processes, in accordance with their own security policy and with a clear segregation of duties. Moreover, all changes within HelloID are recorded, including details on who requested the change, who approved the request and the exact changes in underlying systems this has led to.

A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	HelloID recognises contextual factors, including the use of a mobile device. Depending on the context, certain capabilities can be blocked or made accessible only after additional authentication. In addition to soft or hard tokens and SMS, HelloID also offers various one-time passwords (OTPs) as a second factor. Specific agreements regarding the use of mobile devices can also be digitally reconfirmed and registered in the personnel file in the HR system. Since HelloID Provisioning can be linked to the HR system, it is possible to consider these factors when issuing accounts or rights to employees.
A.6.2.2 Teleworking	HelloID recognises contextual factors, including access from external network environments. Depending on the context, certain capabilities can be blocked or made accessible only after additional authentication. In addition to soft or hard tokens and SMS, HelloID also offers various one-time passwords (OTPs) as a second factor.
A7. Human resource security	Naturally, employees must be sufficiently trained and aware of the importance of information security. This is true for the entire employment relationship, from the proper recruitment of employees to the necessary security measures when people leave the organisation.
A.7.2.1 Management responsibilities	A change in employment often results in a different role with different obligations and rights. These changes are processed in the HR system and, thanks to the integration with HelloID, automatically lead to alterations in roles and access rights for the relevant user. Upon the termination of the employment relationship, obligations for the former employee (such as confidentiality) are enforced because access rights are also automatically terminated.
A.7.2.2 Information security awareness, education and training	Thanks to the structured identity management within HelloID, with clear roles and associated rights, users are working in accordance with the rules automatically, intuitively and safely. This can reduce the need for training. Of course, training agreements and results can also be digitally reconfirmed and registered separately in the personnel file in the HR system. Since HelloID Provisioning can be linked to the HR system, it is possible to take these into account when issuing accounts or rights to employees.
A.7.2.3 Disciplinary procedure	If the outcome of disciplinary procedures leads to the revocation of privileges in someone's HR file, this can automatically lead to restricted access rights thanks to the link between the HR system and HelloID.
A.7.3 Termination or change of employment	

A.7.2.3 Disciplinary procedure	A change in employment often results in a different role with different obligations and rights. These changes are processed in the HR system and, thanks to the link with HelloID, automatically lead to changes in roles and access rights for the relevant user. When employment is terminated, obligations for the former employee (such as confidentiality) are reinforced because access rights are also automatically terminated.
A8. Asset management	Business assets used for processing information (such as software and computer systems) must be well registered and managed. Who is allowed to use the systems, and are business assets and user rights returned upon the termination of activities? All information must be properly classified and stored securely.
A.8.1.1 Inventory of assets	HelloID automatically maintains a registration of digital assets (such as applications and shares) that employees have access to. In addition, HelloID helps to automate the processes for the issuance of physical devices such as laptops and mobile phones.
A.8.1.3 Acceptable use of assets	VThrough the authorisation matrix, each user's role is documented and implemented, with the corresponding access rights for applications and data. Naturally, the agreements regarding the use of assets can also be digitally reconfirmed and registered separately in the personnel file in the HR system. Since HelloID Provisioning can be linked to the HR system, it is possible to take these into account when issuing accounts or rights to employees.
A.8.2.3 Handling of assets	In the case of optionally requestable assets with different classification levels (Availability, Integrity, Confidentiality), various forms of authentication (MFA) and corresponding workflows can be deployed.
A9. Access control	
A.9.1.2 Access to networks and network services	Through provisioning, each employee receives their own personal account. An authorisation matrix can define precisely which network services the user is allowed to use in the context of their work activities within the organisation. When determining access rights, HelloID can also consider contextual factors, such as the use of a mobile device and whether it is an authenticated or unauthenticated device ('bring your own device').
A.9.2.1 User registration and deregistration	Thanks to the provisioning feature, the provision of user accounts can be synchronised with, for example, the registration of employees within the HR system. Additionally, separate registration procedures can be added (for example, for guest accounts). HelloID prevents the use of group accounts and contributes to a conclusive formal administration of user identifications.
A.9.2.2 User access provisioning	By having the organisation work with established roles and mandates and aligning these with HelloID, employees can be given the rights specific to their role(s) at any time. A.9.2.3 describes how to deal with exceptional situations, including special rights.

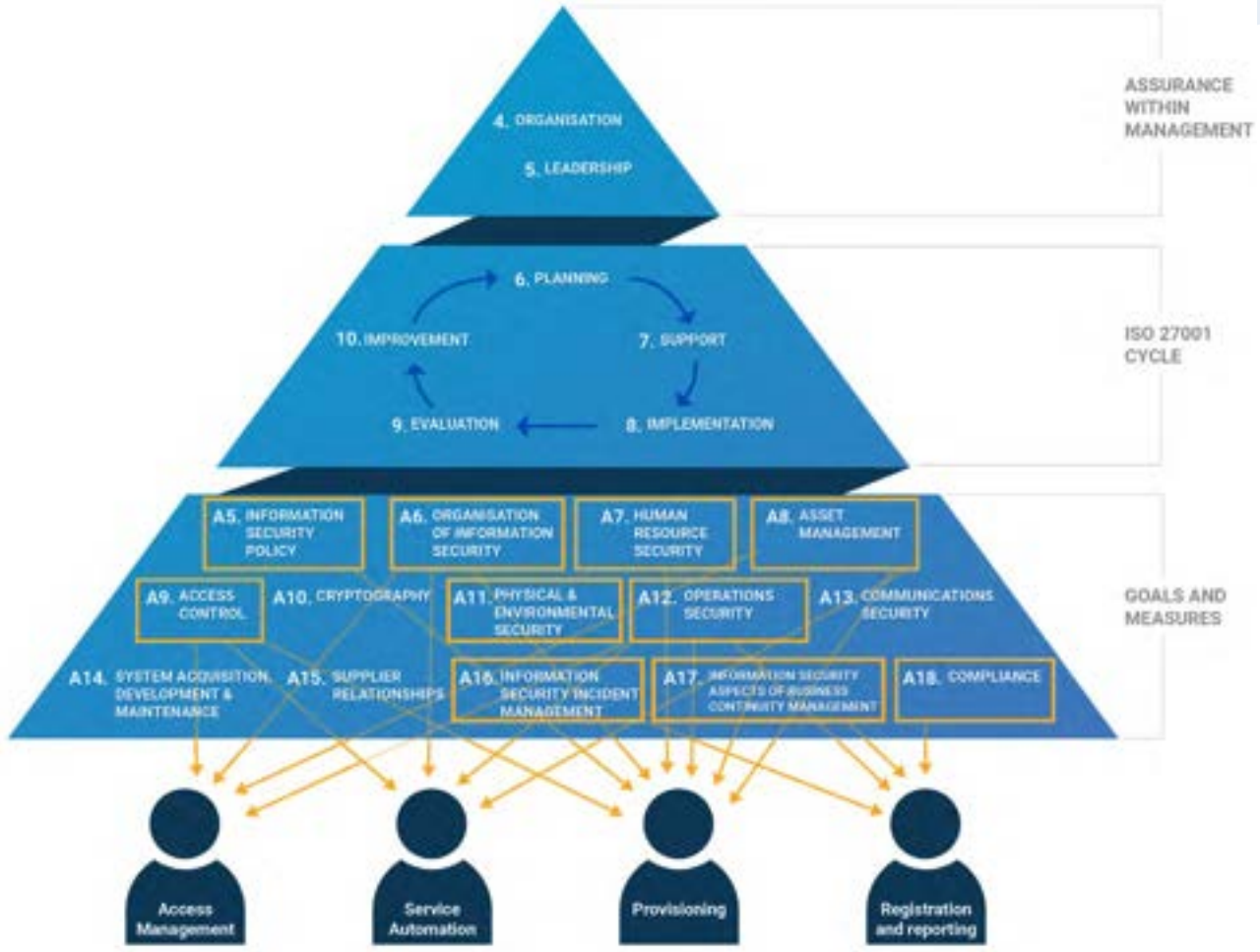
A.9.2.3 Management of special access rights	When it comes to assigning special rights (in addition to general role-based rights, including more privileged rights), rights can be granted on an individual basis. The processes for this can be configured in a client-specific way, including approval procedures (by one or several officers) and regular review thereof.
A.9.2.4 Management of secret authentication information of users	HelloID provides an automated and secure procedure for the initial issuance of secret authentication information (dependent on the organisation, to the private email address or to the manager). The authentication information is then encrypted and stored in an Identity Provider (IdP). HelloID can act as an IdP itself, but it is more common for HelloID to use existing IdPs such as the local Active Directory or Azure AD. Further use of authentication information for other used applications can be limited with single sign-on. This involves the use of tokens between the IdP and service provider.
A.9.4.2 Secure login procedures	HelloID ensures that people always use the required login procedures, supplemented with second-factor verification if necessary. In addition, separate registration procedures can be implemented for special user groups such as guests or suppliers.
A.9.4.3 Password management system	This is often part of the implemented Identity Provider (IdP). If HelloID is used as the IdP, the management processes can be set up in such a way that they comply with the organisation's established password policy (with guidelines on, for example, password length and complexity, the validity duration of the password, etc.).
A10. Cryptography	Data must be sufficiently encrypted to guarantee both the confidentiality and the integrity of the data.
A11. Physical and environmental security	Organisations must prevent unauthorised access to computers and data carriers at office locations. This also means that in the event of a power failure or a calamity, the information security must remain intact. And upon disposal of equipment, the data must be removed.
A12. Operations security	There must be clear agreements and procedures in place that dictate how to use information systems safely and to protect the systems against malware. In addition, clear backup and monitoring measures are required.
A.12.1.2 Change management	Role and rights changes are automatically carried out according to a set process. We proactively monitor for (unexpectedly) high numbers of changes. In such cases, review and approval by an administrator are requested (the thresholds are adjustable). This prevents, for example, an organisational change from leading to significant security risks.

A.12.4.1 Event logging	Logging and reporting are fundamental components of any security policy. Because Identity Management plays a role in many processes, it is crucial that all IdM activities are logged. HelloID takes care of this and provides an 'audit trail' that provides insight into the use of the HelloID environment. All actions carried out within and by HelloID are saved in the Elastic reporting functionality, which has extensive reporting capabilities. The stored information is sufficient to trace incidents back to individual users, the device used, the date and time, and the outcome of the action. This includes, among other things: Provisioning: for each system and user, all actions related to creating, enabling, updating, moving, disabling and deleting accounts, and granting and revoking permissions. Service Automation: all (self-)service actions regarding requests, workflows, approvals, form data and configuration changes. Access Management: all successful and failed login attempts, the geographic location of the user, devices used, initiated password resets, access attempts for applications and access attempts that failed as a result of the access policy. Of course, HelloID can also share the reports and logs with SIEM and/or SOC facilities of the client.
A13. Communication security	Both the internal network facilities and the external network communication must be secured against unauthorised access and misuse.
A14. Acquisition, development and maintenance of information systems	Organisations must consider the security of systems and data during the procurement, development and management of IT systems. This does not only concern operational systems. Development, demonstration and test systems must also be adequately secured.
A15. Supplier relationships	Organisations are dependent on suppliers for their IT systems. This applies to both systems and software delivered on-premises and suppliers managing sensitive cloud data. Clear agreements with suppliers are necessary to guarantee information security.
A16. Information security incident management	Despite all security measures, an incident can still occur. To deal with this, there must be solid procedures with clear responsibilities in place, including agreements on further reporting and resolution.

A.16.1.7 Collection of evidence	All access attempts are recorded within the HelloID Identity Management platform. The platform also provides an overview of each user's access rights at any given time. In addition to role-based rights, the system can track all exceptions (who requested specific access rights and who granted approval). All registered data can be stored and/or shared with other client systems, in accordance with the client's security policy.
A17. Information security aspects of business continuity management	In the event of incidents involving the IT facilities, it must be specifically ensured that the continuity of information security is always guaranteed.
A18. Compliance	As an organisation, you must continuously be able to demonstrate that you comply with all applicable laws and regulations.

Identity Management and ISO 27001

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



Provisioning of user accounts and rights

Within ISO 27001, group accounts, as well as the 'copy user' principle for new incoming employees, are not acceptable. These days, access rights must be unequivocally linked to individual user accounts. It must be clear at any given time who has access to certain data and applications and who carries out certain actions. And of course, the account details and access rights must always be up-to-date, meaning 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 meeting these requirements.

Within HelloID, we safeguard this through automated provisioning. Thanks to this feature, someone's digital identity and access rights are always aligned with the information as registered in the HR system. Thanks to a direct link between the HR system and HelloID, the new employee receives a user account with associated facilities and rights that fit their role immediately upon onboarding. We also keep this automatically updated throughout their tenure. If someone's role changes, HelloID promptly adjusts the access rights. And when 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 remain accessible by mistake is no longer possible.

Service Automation: standardisation with room for exceptions

Good information security relies on clear policy rules, transparent processes and little room for individual and uncontrolled customisation. To ensure this, we aim to standardise and automate identity management processes as much as possible. While supporting concepts like role-based access and implementing processes with a clear division of roles, there will always be exceptions, and every organisation must find its own balance between user-friendliness and business security. Automatically providing too many rights leads to unwanted security risks. However, unnecessarily making employees wait for their access rights hinders their work.

HelloID offers the desired combination of standardisation and exceptions:

- Standardly within HelloID, rights can be assigned with the help of the so-called Attribute Based Access Control (ABAC) functionality. We use HelloID to help translate the organisational structure, including roles and corresponding tasks, into configurable business rules that automatically determine which access rights an employee gets. From the automatic onboarding at the start of employment to the departure procedure upon leaving.

- The majority of the rights are thus fully automated, but a standard role matrix is never completely comprehensive, and therefore HelloID also provides for exceptions. For more specific and more difficult to automatically distribute rights, you can design self-service processes. Users can themselves request online access to applications or data shares, with the correct approval steps automatically being followed. Following approval, the automated process ensures further activation without risky exceptions or mistakes.

Automated configuration rules ensure that the services catalogue remains automatically up-to-date. For example, a new share immediately becomes visible in the catalogue. At any moment, 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, if necessary, partners and customers - get easy and uniform access to applications and data. As explained before, the principle is that each user is equipped with one personal user account. With a concept like 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 per application. For access to applications without built-in SSO capabilities, HelloID offers alternative methods to ensure 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 recognizes contextual factors such as the login location and time and may ask the user for additional authentication based on these. Alongside 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 with the advantage of lower investments, quick installation and configuration. Tools4ever handles the technical management, including automatic updates. The solution is implemented using highly secure Microsoft Azure and Google Cloud environments, which are also thoroughly checked every six months by Deloitte Risk Services. Compliance with strict security requirements is therefore guaranteed. The service also has very high availability thanks to built-in redundancy.

Reporting

For ISO 27001 compliance, registration and reporting are essential. As an organisation, you must be able to demonstrate that the various processes comply with relevant laws and regulations. You must also be able to trace which users within the network have performed which actions, in the event of a security incident such as a data breach.

As a cloud-based solution, HelloID must meet increasingly stringent laws and regulations regarding audits and security. All access attempts, automated and manual processes, and the use of our platform are therefore recorded and made transparent.

This ensures the authentication process is automatically monitored. The reports always ensure

clarity into who has accessed which applications, at what time and from which location. This not only provides a detailed view of the authentication journey but also shows, for example, login attempts from suspicious IP addresses. Potential threats can be identified in time to take countermeasures.

What is particularly distinguishing is that within HelloID the complete identity lifecycle per system and per user is auditable. All executed actions are logged, such as creating, enabling, updating, moving, disabling and deleting accounts. The same applies to the granting and revoking of permissions. If rights are granted ad hoc (outside the regular role matrix), it is possible through HelloID to see exactly who requested this, who approved the request, as well as the precise changes in underlying systems this has led to. As a result, the HelloID process is fully transparent, verifiable and adaptable.

Want to know more?

These days, Identity Management plays a central role within your IT security. Employees, partners and customers should only gain access to applications and data with their own account on a 'need to know' basis. Moreover, we must be able to trace all IT activities back to the level of individual users. This makes your Identity Management platform a key element in setting up your ISO 27001 compliant information security system.

Want to know more about the role Identity Management can play in ISO 27001 compliance within your organisation? And how can you keep your IT environment safe without compromising on user-friendliness? We are happy to tell you more about this. For example, by means of our ISO 27001 – HelloID checklist. In this list, we address all ISO 27001 Annex A measures with an explanation for each measure on whether – and, if so, how – HelloID Identity Management can contribute.

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