



Compliance with Doxis

Good reasons for certified ECM software



Are you about to launch an enterprise content management (ECM) system? Do you want to replace your existing archive or DMS with a true ECM system that brings together all functions, from archiving to DMS and BPM, onto one single platform? Then you'll quickly find yourself dealing with a myriad of legal requirements and vendor specifications that have to be fulfilled!

In this situation, certifications can offer you orientation and security: They attest to an ECM software's compliance with legal guidelines and industry standards and offer full support and secure communication for production systems such as SAP and Microsoft.



Maintain the validity of your information	4
Avoiding tax setbacks	4
Storing tax-relevant documents in Germany	4
Protecting personal data and building trust	5
 The US discovery process	 6
US law versus European data protection	6
Recommended organizational measures	6
The importance of storage and deletion concepts	6
 The value of certified ECM software	 7
The advantages of certified ECM software	7
Recommended organizational measures	7
 Adhere to laws, standards and more with Doxis	 8
Certified security with Doxis	9
Foundational protection	10
Uphold laws and regulations	10
International laws and regulations	10
Domestic laws and regulations	11
Extended security	15
Meet standards, norms and guidelines	15
International standards, norms and guidelines	15
Domestic standards, norms and guidelines	17
Compliance on top	19
Vendor certifications	19
Fill out your ECM compliance checklist!	20
 Your certified partner for future-proof solutions	 21
Doxis' ISO certifications for quality management & information security	21

Maintain the validity of your information

Information is proof. It serves as evidence in court hearings — for example, for damage claims or as documentation in a regulated environment. In situations like these, the validity of evidence is put into question. Software certifications and system/access documentation can demonstrate that information has not been retroactively manipulated.

Software certificates are a must in e-business. One of the key components of an information management system are certifications which attest to the security of your information storage and data transfers. If you want to practice reliable digital information management, you need secure tools and methods. With certified ECM software such as Dosis, you get demonstrable assurance that, if used appropriately, your company will always be able to prove and maintain the validity of your information.

Avoiding tax setbacks

Invoices, contracts, order confirmations, annual reports: Certain information must be stored according to legal requirements. For example, lawmakers require that you archive tax-relevant data and documents for specific retention periods. In some companies, invoices may have to be stored for ten years. Some say that original documents are not allowed to be destroyed during this period. This is wrong!

That's why it's so important to make sure that digital documents used as evidence or for auditing are stored in an audit-proof way. Certified ECM software such as Dosis gives you the means to accomplish this. Presenting auditors a certificate for your software is typically sufficient proof that principles such as immutability and completeness of tax-relevant documents have been fulfilled. This means you are prepared for the next audits.



**Dosis ensures
constant
accountability
and traceability!**

Legal retention periods often applies to:

- books and recordings
- annual reports
- status reports
- accounting documents
- invoices
- and more

Protecting personal data and building trust

Personal data must be well protected. And the European Union has put this into a law: New data protection requirements have been added to the EU General Data Protection Policy (GDPR). The content of the new EU regulations affects your customers and partners in that, effective immediately, they have more rights. For you this means that, in addition to protecting personal data (Art. 32, EU GDPR), you must now also fulfill a person's right to erasure (Art. 17, EU GDPR) or the right to data portability (Art. 20, EU GDPR). If you fail to do so, you may be subject to penalties of up to 20 million euros or up to 4 percent of your company's total revenue (whichever is higher).

Are you able to fulfill these requirements with your preferred ECM system? EU GDPR certification can provide you orientation. A certified ECM software such as Dosis can help you to process, store, transmit and delete personal data in a traceable way and in compliance with the EU GDPR.

For more information about the EU GDPR certification of Dosis, please see page 10.

Excerpts from the EU GDPR

Art. 17 – EU GDPR: The right to erasure

The data subject has the right to request that the data controller immediately erase personal data.

Art. 20 – EU GDPR: The right to data portability

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format.

The US discovery process

International companies need to manage diverse legal requirements of the countries in which they operate. In the US, before civil litigation takes place adverse parties are obligated to exchange information and documents. Upon court disposition, companies must provide all requested information to the extent that it is available. The purpose of this is to provide material evidence, which can also include information that may negatively expose a company — for example, trade secrets or confidential documents.

It's not just emails

Disclosure requirements regarding the required data are quite extensive. All electronically stored information that is connected to the dispute subject is considered evidence. This includes:

- Emails/correspondence
- Voice messages
- Photos
- Tables
- Notes
- And more

Companies based out of Europe, particularly those with US subsidiaries, are also affected by this. According to federal procedural rules, non-US companies may be required to provide information, including personal data. Beyond having a firm grasp of the legal situation in the US, it is imperative that companies also have systematic archiving practices in place, which include the deletion of documents. If information is unlawfully deleted, penalties are possible under US law.

US law versus European data protection

US and European legal regulations couldn't be more different. European laws stipulate that companies must archive as many business documents as possible to meet legal compliance requirements. From an e-discovery perspective, companies face the challenge of deleting information as quickly as possible to avoid having to provide it in litigation.

Recommended organizational measures

Companies that do business on both sides of the Atlantic have to balance a legal high-wire act: On the one hand, they must archive business and tax-related documents for a specific time period. Being able to demonstrate to courts and tax authorities that information can be retrieved at any time and that it is securely, completely, compliantly, immutably and reproducibly stored and managed without losses — all this creates a foundation of trust. On the other hand, information that no longer serves the interests of a company should be deleted. This high-wire act requires a deletion concept that conforms with data protection laws. This means that if you don't need it, it has to go. Conversely, this also means that what no longer exists cannot be submitted or seized.

The importance of storage and deletion concepts

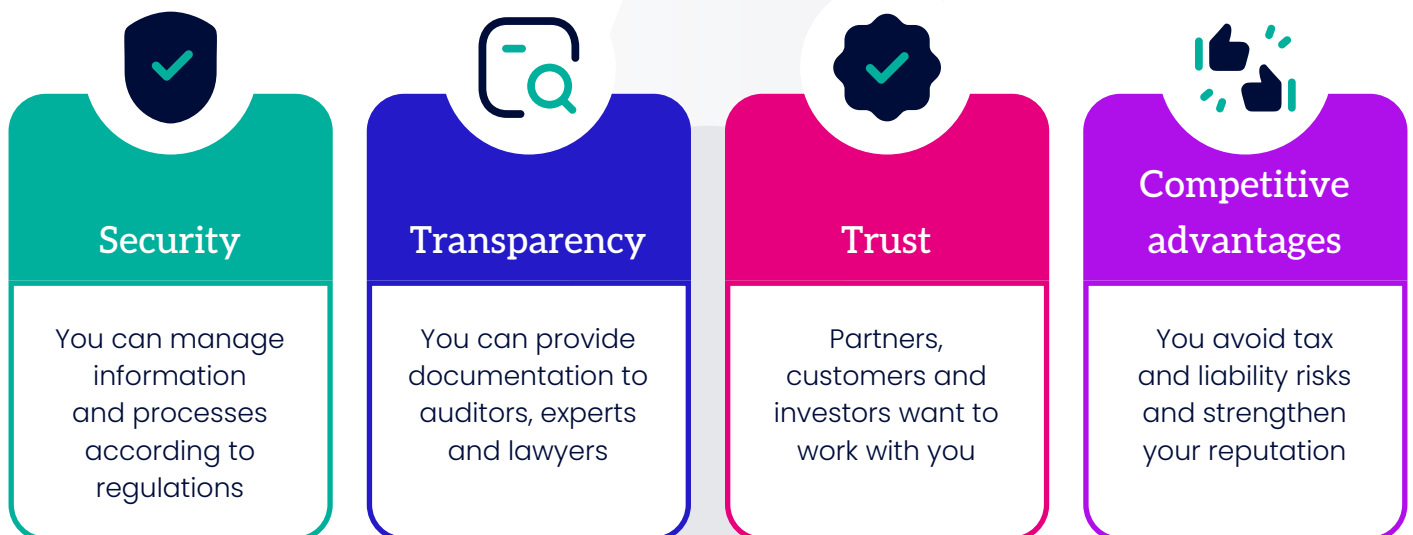
Certified and company-wide ECM software that adheres to retention and deletion guidelines is recommended for companies that store digital information across various data pools. Such software also helps companies to control large amounts of data. One of the first organizational measures of a company should be to define how information should be accessed and identified and to create a retention and deletion concept that complies with legal requirements.

The value of certified ECM software

Certifications provide security: With certified ECM software such as Dosis, you can fulfill the technical and organizational requirements of domestic and international laws, regulations, norms and standards when processing information. With our Dosis certifications, you are able to demonstrate to auditors, experts and lawyers that you deploy software that stores business and tax-related documents in an audit-proof way, that is able to create documentations in compliance with the law, and that offers sufficient protection from digital manipulation, loss and theft.

You can also demonstrate to your customers, suppliers and investors that your information and processes are managed in compliance with laws and regulations. This builds trust and improves your reputation! If people know they can rely on your accounting, profit forecasts, data protection measures, etc., then the decision to work with you will be made even faster.

The advantages of certified ECM software



Adhere to laws, standards and more with Doxis

Doxis is a certified ECM software that fulfills the technical and organizational requirements of legal regulations. Independent auditors have confirmed this in their certificates and attestations regarding the correct usage of Doxis in combination with certain organizational checks. It is ultimately your responsibility to correctly use the Doxis software and to have the correct configuration options to properly meet legal regulations applicable to you.

Regulations form the basis of legal compliance. Doxis and its certifications provide you a **comprehensive** technical and organizational **foundation of protection**.

The fulfillment of standards, norms and guidelines are important prerequisites for many business relationships. Doxis certifications provide you **even greater security** to meet these requirements.

What happens to all the other information that is generated in systems outside of your ECM system? Doxis has a huge benefit here: Thanks to **vendor-certified interfaces**, you can integrate this information securely into your ECM system, where you can efficiently and consistently manage it.

When you choose to work with Doxis, you also choose an ECM system that is audited and certified according to the highest security standards!

“ With certified ECM software like Doxis, companies can more easily prove the audit-proof status of their information, avoid risks, create trust and strengthen their reputation!

Dr. Gregor Joeris
Chief Technology Officer, Doxis

Certified security with Doxis

On the following pages, we give you an overview of the certificates and attestations that Doxis offers on the international and national levels in the contexts listed below.



Extra security

Make sure that you have complete support for vendor specifications and secure communication through vendor-certified interfaces.



Extended security

Fulfill standards, norms and guidelines.



Foundational protection

Demonstrably uphold laws and regulations.



Foundational protection

Uphold laws and regulations
International laws and regulations



EU GDPR

The EU GDPR is a legal regulation that harmonizes the rules according to which companies and public authorities across the EU handle personal data. The regulation applies to companies that collect, process, store, transmit and analyze personal data. These kinds of processes also take place in an ECM system. That's why it's so crucial that companies can prove that their data processing is compliant with the EU GDPR.

The auditing firm Ebner Stolz **has certified Dosis as the first ECM software worldwide to fulfill the EU General Data Protection Regulation (GDPR)**. With Dosis, companies can

- protect,
- traceably delete,
- transmit and
- make available
- personal information according to the EU GDPR.

This means that companies fulfill important requirements such as the right to erasure (Art. 17, EU GDPR), the right to data portability (Art. 20, EU GDPR) and the secure processing of personal data (Art. 32, EU GDPR).

Find out how Dosis can help you to comply with the EU GDPR:

www.dosis.com/en/business-platform/certification/eu-gdpr





Foundational protection

Domestic laws and regulations

**GoBD**

In Germany, the principles for the proper management and storage of books, records and documents in electronic form as well as data access (GoBD) lay out the rules for the accounting and storage of tax-relevant electronic data and paper documents in digital form. They apply to all data-processing systems. The principles of GoBD therefore also apply to an ECM system.



The auditing firm Ebner Stolz **has certified that the ECM software Doxis is compliant with GoBD**. The suitability of the software for the fulfillment of the GoBD principles was tested. This included

- Traceability and auditability
- Completeness
- Accuracy
- Orderliness
- Immutability
- Machine-based analysis capability
- Scanned paper documents
- Documentation framework

Procedural documentation

According to GoBD, each data-processing system must have a procedural documentation, which enables a company to document the content, the structure and the results of a data-processing procedure. This covers, for example, processes in connection with the storage of tax-relevant data and documents.



Foundational protection

Domestic laws and regulations



IDW PS 880

In addition to GoBD in Germany, there is also the commercial code (Handels-gesetzbuch; HGB) and the fiscal code (AO) that pose further requirements on the audit-proof digital archiving of documents subject to commercial and tax law. This includes documenting, processing and storing business documents. Information-processing systems that pass the auditing standard 880 of the Institut der Wirtschaftsprüfer (IDW PS 880), the German institute of auditors, fulfill these requirements. With the **IDW PS 880 certification**, the auditing firm Deloitte & Touche certifies that electronic archiving with Dosis can be performed audit-proof according to GoBD, the commercial and fiscal code.



§ 14 (1) German Value-Added Tax Act

The German Value-Added Tax Act, § 14 (1) specifies the requirements for the proper processing and archiving of inbound and outbound electronic invoices. **Based on the IDW PS 880 certification**, the auditing firm Ebner Stolz certifies that Dosis enables companies to process inbound invoices according to the law.



MaRisk/KWG

The Minimum Requirements for Risk Management (MaRisk) are administrative directives issued in a circular of the Federal Financial Supervisory Authority (BaFin). They provide a framework for German financial institutes to structure risk management. They are based on § 25a of the German Banking Act (KWG). This also covers requirements regarding quote processes, which are comparable to those of the internal control system (IKS) and of an internal audit. They stipulate, for example, that business processes, organizational structures and procedures must be documented, included in the written rules of procedure, announced and made accessible to the employees. Dosis supports financial and credit institutions in fulfilling these requirements **in compliance with the law.**



Foundational protection

Domestic laws and regulations



Banking Supervisory Requirements for IT (BAIT)

The Banking Supervisory Requirements for IT (BAIT) were published on 06.11.2017 with Circular 10/2017 (BA). They specify the minimum requirements for risk management contained in MaRisk and are the central building block for IT supervision in the banking sector. Among other things, they require banks “to base the design of their IT systems and associated IT processes on common standards. These include, for example, the IT basic protection catalogs of the Federal Office for Information Security and the international security standard ISO/IEC 2700X of the International Organization for Standardization.” **Dosis supports banks and credit institutions in meeting these requirements in a BAIT-compliant manner.**



AktG

In the German Stock Corporation Act (Aktiengesetz), § 91 addresses the organization and accounting of a public limited company. It stipulates that the management board must practice proper risk management. This includes the obligation to conduct legally compliant archiving of electronic data and documents – with safeguards against data theft and loss. These safeguards must also be documented. **With Dosis, companies are able to fulfill these technical requirements according to the law.** You can set up, document and always be able to demonstrate the required safeguards for electronic archiving.



WpHGt

According to § 15b of the German Securities Trading Act (WpHG), publicly listed companies are required to maintain lists of persons working for them who have access to inside information as a part of their function. Regardless of whether the lists are in paper form or digital: This personal data must be complete, always accessible and available to legal authorities within a reasonable time period. **Dosis enables companies to fulfill these WpHG requirements.**



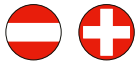
SRVwV

The SRVwV, the general administrative regulation on accounting in the social security system, places requirements on the electronic archiving of providers of statutory accident funds and of statutory health, accident and pension insurances. The legal authorities demand, for example, that certain documents of a scanning process be labeled with qualified signatures. **Dosis makes it possible to provide electronic signatures in compliance with SRVwV.** The providers can therefore document and prove the proper conversion of paper documents into digital format.



Foundational protection

Domestic laws and regulations



Audit security in Austria & Switzerland

The generally accepted accounting principles (e.g. truth, transparency, completeness) are legally regulated in German-speaking countries. In Austria, this is covered by the öBAO, the Austrian tax code. **Doxis makes it possible to meet all of the related legal regulations.** It enables companies to file internal documents in an audit-proof and transparent way. Using an ECM system, companies can structure all information clearly, simply and completely to provide it to auditors and supervisory authorities.

In Switzerland, there are three main federal regulations: the GeBüV, which are accounting regulations; the OR, the code of obligations; and the EIDI-V, the federal department of finance regulation regarding electronic data and information. All three place requirements — e.g. transparency, completeness or providing supporting documents — on how companies manage and archive information that is subject to retention. **Doxis conforms with these domestic legal regulations.** Companies can fulfill the requirements and are able to demonstrate compliance at an auditor's request.



SOX (Sarbanes-Oxley Act)

The SOX is a US federal law that requires, among many things, that electronic documents, particularly emails, of companies publicly listed in the US stock exchange comply with a set of regulations. This also applies to non-US companies that trade securities on a US stock exchange, to non-US subsidiaries of US companies and to suppliers of companies subject to SOX. **Doxis conforms with these legal requirements regarding electronic storage.** Companies subject to this are thereby capable of meeting them.



Extended security

Meet standards, norms and guidelines
International standards, norms and guidelines

SOC 1–3 certification

Dosis Cloud Services have been successfully certified according to the international SOC 1 Type 2, SOC 2 Type 1 & 2 and SOC 3 standards, confirms the independent auditing firm CyberGuard Compliance LLP in its audit report. A “type 1” certification refers to the successful testing of the control system itself. In receiving the SOC 2 Type 2 certification we continuously and fully demonstrate in annual reviews that it consistently applies the **effective controls and processes, to ensure the highest level of security and availability in the cloud.**



ISO 14641-1:2012-02

The specifications regarding the design and operation of information systems for securing electronic documents pose a number of organizational procedures and technical requirements regarding the capturing, storage of and access to electronic documents and processes. **Dosis is certified for this norm.** What does this mean for your company? The information you store in Dosis fulfills rigid security standards and is protected from digital manipulation and unauthorized access.

ISO 14721:2012 (OAIS)

The ISO standard 14721 for an Open Archival Information System (OAIS) is the reference model for long-term digital archiving. It describes seven functional entities with over 50 functions and 40 interactions to which an OAIS-conforming archive must abide. **Dosis conforms with this.** With the help of audit-proof Dosis archiving, companies can fulfill the defined requirements regarding the long-term or permanent storage of their digital information.

ISO 15489-1:2016

The guidelines for records management in public and private organizations provide quality standards for international records management and provide an outline for transparent and traceable administrative and business processes. **International firms are able to conform to ISO 15489-1:2016 with Dosis.**



Extended security

International standards, norms and guidelines

ISO 16175:2020

The ISO standard 16175:2020 describes the principles and functional requirements for records in digital business operations. **Dosis is certified for this standard.** Companies are therefore able to fulfill 275 cross-industry requirements such as capturing, management, storage and deletion of information.



MoReq2010

The Model Requirements for Records Systems (MoReq) are European cross-industry specifications for electronic document, archive and records management. We contributed our own experience from developing eGovernment solutions to co-authoring the MoReq. The MoReq2010 forms the basis for various European standards, e.g. in public administrations in England, The Netherlands, Luxembourg and Norway. **Dosis conforms with this.**

Basel III

Basel III refers to capital and liquidity requirements for banking institutions and replaces Basel II. Among other things, the new regulations are intended to increase the capital base of institutions and thus better protect banks and financial institutions against future crisis situations. Based on a bank's own ratings or external ratings, the credit rating of borrowers is systematically assessed using their business data. This assessment also factors in business and communication documents (e.g. emails), which banks must document, store and protect from misuse. **Dosis enables companies to fulfill these requirements of Basel III.**





Extended security

Domestic standards, norms and guidelines



DoD 5015.2

The 5015.2 standard of the US Department of Defense (DoD) defines requirements for records management within the Department of Defense, which has also become the accepted standard for many state, county, and local governments in the US. **Doxis conforms with DoD 5015.2 requirements** and is used by companies to meet this standard.



FDA 21 CFR Part 11

The US Food and Drug Administration (FDA) sets requirements for electronic recordings and signatures in Part 11, Title 21 of the Code of Federal Regulations (CFR). This applies to documents that prove the fulfillment of regulatory obligations in the US food and drug industry. **Doxis conforms with these requirements.**



HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. law that establishes requirements for the handling of Protected Health Information (PHI). **Doxis conforms with these requirements.**



FERPA

The Family Educational Rights and Privacy Act (FERPA) is a U.S. federal law that protects the educational records of students. **Doxis conforms with these requirements.**



CCPA

The California Consumer Privacy Act (CCPA) requires companies that process the data of California residents to ensure transparency and data security. Key requirements include users' rights to access and delete their data, a "Do Not Sell" link for data sales, and updated privacy policies. **Doxis conforms with these requirements.**



Extended security

Domestic standards, norms and guidelines



NEN 2082

In The Netherlands, NEN 2082 is a standard that applies to digital archiving in public sectors. It is based on standards such as MoReq and DoD 5015.2 and covers 155 requirements pertaining to the functionality of information and records management software. **Doxis is NEN 2082-certified.**



NF Z 42-013

In France, the association française de normalisation (AFNOR) has specified in norm NF Z 42-013 how electronic archive systems should be designed, which system components they must include and how they operate. The norm is based on the ISO standard 14641-1:2012. With this ISO certification, **Doxis also conforms with NF Z 42-013.**



EHA 962/2007

In Spain, the Ministerio de Economía y Hacienda has issued the EHA 962/2007 regulations regarding electronic invoicing and the storage of electronic invoices. **The ECM system Doxis conforms with this** and thereby helps companies to fulfill this invoicing regulation.



FSTEC

The Russian Federal Service for Technical and Export Control (FSTEC) only permits companies to do business in the Russian IT market if they fulfill certain guidelines and regulations regarding exports and software technology. One aim of these rules is to prevent unauthorized data and information access. **Doxis is FSTEK-certified** and permitted in the Russian market.



GOST

The Gossudarstvennyy (GOST) standard is a federal Russian norm that stipulates quality and security requirements on products. **With the FSTEK certification, Doxis also conforms with the following standards.**

- GOST 2.114-95
- GOST 19.202-78
- GOST 19.402-78
- GOST 19.502
- GOST 2.610-2006
- GOST 19.401-78
- GOST 19.501-78



Compliance on top

Vendor certifications

SAP-certified integration

A vendor knows that its ECM software is successfully integrated with SAP when SAP certifies its SAP interfaces and add-ons.

Over seventy percent of our customers use Doxis together with SAP. The two solutions mesh seamlessly. This is guaranteed by regular (re-)certifications of Doxis' SAP interfaces and SAP add-ons: for all SAP data and document archiving functions, electronic files in SAP and SAP invoice processing.



Doxis has the following SAP certifications

- The Doxis SAP ArchiveLink interface is certified by SAP for the S/4-BC-AL 7.40 integration scenario.
- The Doxis CMIS Connector interface is certified by SAP for SAP BTP Document Management Service in the cloud.
- The Doxis interface for ILM and retention with SAP S/4HANA is certified according to SAP specification S/4-BC-ILM 1.0.
- Doxis Document Management for SAP SuccessFactors is certified for integration with SAP SuccessFactors Employee Central & Recruiting according to SAP integration scenario SFSF-INTEG 1.0.
- Doxis Document Management for SAP S/4HANA has been certified for use on SAP S/4HANA Cloud Private Edition, Release 2023, via the SAP integration scenario S/4HC-ABAP-COND.
- In its certificate, SAP confirms the successful integration of Doxis Purchase-to-Pay Automation for SAP S/4HANA (AFI Invoice 5.0) via the SAP integration scenario Add-On Deployment for Rise with SAP.
- In its certificate, SAP confirms the successful integration of Doxis Purchase-to-Pay Automation for SAP S/4HANA (AFI Confirmation 5.0) via the SAP integration scenario Add-On Deployment for Rise for SAP.

SAP® Certified
Integration with SAP® S/4HANA

SAP® Certified
Built on SAP Business Technology Platform

SAP® Certified
Integration with SAP® S/4HANA

SAP® Certified
Integration with Cloud Solutions

SAP® Certified
for clean core with SAP S/4HANA Cloud

SAP® Certified
Integration with RISE with SAP S/4HANA Cloud

SAP® Certified
Integration with RISE with SAP S/4HANA Cloud

SAP® Certified
Integration with RISE with SAP S/4HANA Cloud



Compliance on top

Vendor certifications**Microsoft**

When software is able to fulfill the stringent integration requirements of Microsoft, the US vendor confers the status of **Microsoft Gold Partner**. Dosis has already been able to achieve this status eleven years in a row. This Gold status is assigned to only one percent of all Microsoft partners. Customers benefit from Dosis' long-term strategy of continuously investing in employee qualification.

Gold
**Microsoft
Partner**

**Dosis is integrated
into the following
Microsoft products**

- Microsoft Office
- Microsoft Outlook
- Microsoft Teams
- Microsoft SharePoint
- Microsoft Dynamics NAV & AX

Every customer has the guarantee that when Microsoft releases new operating systems and databases (e.g. Windows and SQL servers), Dosis can immediately be run on them.



Which legal requirements, industry standards and vendor specifications do you want to meet and cover with your ECM software?

Request your own ECM compliance checklist for information management right now!

info@dosis.com

Your certified partner for future-proof solutions

Doxis' ISO certifications for quality management & information security

ISO 9001:2015 (quality management)

Our development subsidiary, Doxis Software Technology GmbH, has been successfully certified according to ISO 9001:2015, the most widely used international standard in quality management (QM). This proves that the software development of Doxis products meets international quality requirements. Standardized processes ensure high-quality software development and documentation. Regular audits monitor compliance with quality standards in all departments. **As an ISO-certified supplier, Doxis is also approved for customers in highly regulated industries without additional audits.**



ISO 27001:2013 (information security management system, ISMS)

Doxis has successfully achieved ISO 27001 certification and received the ISO certificate from the international certification body ABS Quality Evaluations, Inc. for its information security management system (ISMS). This certification of Doxis' ISMS proves that our information management system meets the highest globally recognized standards for the security of business, customer and employee information. **The certification of Doxis' ISMS is proof that its information management system for securing these types of information meets the highest globally recognized standards.**





www.doxis.com