



**Datum:** 7. August 2025

**Veröffentlichung:** Nur für den internen Gebrauch



**Durchgeführt von:** Thomas Werner- Lead Auditor

**Start:** 17.07.2025 - 12:00 Uhr



**Verantwortlich:** DICIS Team, Dirk Sommer

**Ende:** 07.08.2025 - 17:00 Uhr

Dieses Audit verfolgt das Ziel, die Konformität und Qualität der Softwareentwicklungsprozesse von CROSSSOFT im Hinblick auf die ISO 9001 und ISO 27001 Standards zu überprüfen. Es soll sichergestellt werden, dass die hohen Anforderungen an das Qualitätsmanagement sowie an die Informationssicherheit erfüllt werden, insbesondere im Kontext der Entwicklung professioneller Softwarelösungen für den Medizin- und Industriebereich. Durch die Analyse der Implementierung und der Effektivität der bestehenden Qualitäts- und Sicherheitsmaßnahmen wird geprüft, inwiefern CROSSSOFTs Produkte und Dienstleistungen den Bedürfnisse und Anforderungen ihrer Kunden gerecht werden. Das Audit wird zudem dazu beitragen, Verbesserungsmöglichkeiten zu identifizieren und die fortlaufende Compliance in einem sich schnell wandelnden Technologiemarkt zu gewährleisten.

Ergebnisübersicht	
Anzahl Ergebnisse	0
Anzahl Abweichungen / Non-Konformitäten	0



## Auditmethodik

Bitte beschreiben Sie, wie Sie dieses Audit durchgeführt haben

### Methodik des ISO 9001 und ISO 27001 Zertifizierungsaudits der CROSSSOFT GmbH (2025)

Die CROSSSOFT GmbH verfolgt eine strukturierte und systematische Methodik bei der Durchführung des Zertifizierungsaudits für ISO 9001 und ISO 27001, um die Konformität und Qualität ihrer Softwareentwicklungsprozesse zu überprüfen. Dies geschieht insbesondere im Kontext der Entwicklung professioneller Softwarelösungen für den Medizin- und Industriebereich. Die Methodik umfasst vier zentrale Kategorien, die im Folgenden näher erläutert werden:

#### ### 1. Dokumentation Überprüft

Zunächst wird ein umfassender Auditprozess eingeleitet, der die Überprüfung der gesamten relevanten Dokumentation beinhaltet. Dabei wird sichergestellt, dass alle dokumentierten Prozesse, Richtlinien und Verfahren vollständig, aktuell und konform mit den Anforderungen der ISO 9001 und ISO 27001 sind. Hierbei werden unter anderem Dokumente zu den Softwareentwicklungsprozessen, Risikoanalysen, Qualitätsmanagementplänen und Informationssicherheitsrichtlinien herangezogen. Die vollständige Dokumentation ist entscheidend, um die Basis für die Analyse und Bewertung zu schaffen.

#### ### 2. Umfassende Analyse

Im nächsten Schritt erfolgt eine detaillierte Analyse der Umsetzung der Anforderungen aus beiden Normen. Hierbei wird der Fokus auf die Implementierung und Effektivität der bereits bestehenden Qualitäts- und Sicherheitsmaßnahmen gelegt. Die Analyse berücksichtigt spezifische Aspekte wie:

- Die Qualität der Softwareentwicklungsprozesse, insbesondere in Bezug auf das Patientenmanagement, die Ressourcenplanung und die Integration des HL7-Enterprise Service Bus.
- Die Implementierung der Sicherheitsmaßnahmen zur Gewährleistung der Informationssicherheit bei der Verarbeitung sensibler medizinischer Daten.

Ziel ist es, den aktuellen Stand der Prozesse zu erfassen und aufzuzeigen, inwieweit diese den festgelegten Qualitätsstandards und Sicherheitsanforderungen genügen.

#### ### 3. Befragung Durchgeführt

Ein wichtiger Bestandteil der Methodik ist die Durchführung von Befragungen relevanter Personen innerhalb des Unternehmens. Dazu zählen Teamleiter, Entwickler und Mitarbeiter, die direkt an den Softwareentwicklungsprojekten beteiligt sind. Durch gezielte Fragen wird ermittelt, wie die Normvorgaben in der Praxis umgesetzt werden und welche Herausforderungen dabei eventuell auftreten. Diese Erkenntnisse sind entscheidend, um die praktische Anwendung der Qualitäts- und Sicherheitsstandards zu verstehen und gegebenenfalls bestehende Lücken zu identifizieren.

#### ### 4. Erfolgskontrolle

Abschließend wird eine Erfolgskontrolle durchgeführt, um zu überprüfen, ob die eingeleiteten Maßnahmen zur Verbesserung der Prozesse effektiv umgesetzt wurden und die gewünschten Ergebnisse erzielt haben. Hierbei werden sowohl qualitative als auch quantitative Daten betrachtet, um die Entwicklung und Verbesserung der Softwarelösungen zu messen. Im Rahmen der Erfolgskontrolle wird auch evaluiert, ob die Nachhaltigkeit der Maßnahmen in einem sich wandelnden Technologiemarkt gewährleistet ist.

Durch diese methodische Vorgehensweise gewährleistet CROSSSOFT, dass die hohen Anforderungen an das Qualitätsmanagement sowie an die Informationssicherheit nicht nur erfüllt, sondern kontinuierlich verbessert werden, um den Bedürfnissen ihrer Kunden im Gesundheitssektor gerecht zu werden. Dies trägt dazu bei, die Compliance sicherzustellen und das Unternehmen in einem dynamischen Wettbewerbsumfeld zu positionieren.

## Zertifizierte Normen

Das Zertifizierungsaudit umfasste die vom Unternehmen umgesetzten und angewendeten Normen

Qualitätsmanagementsystem nach ISO 9001:2015

Informationssicherheitsmanagementsystem nach ISO 27001:2022

## Auditplanung

Ablauf des Zertifizierungsaudits

Das Zertifizierungsaudit erfolgte nach dem folgenden dem Management vorab mitgeteilten Plan. Die Auditzeiten richteten sich nach den in ISO 17021 und ISO 27006 definierten Anforderungen. Die Grundlagen der Kalkulation sind in den DICIS Zertifizierungsrichtlinien festgehalten, deren aktueller Stand auf der DICIS-Webseite öffentlich eingesehen werden kann.

Stufe	Inhalt	Methodik
Vorgespräch	Mitteilung der Auditziele, des Vorgehens und der Methodik	Managementmeeting
Stufe 1 Audit	Überprüfung der Dokumentation: Einhaltung der Vorgaben von Kapitel 7.5, Überprüfung der Vollständigkeit der Inhalte	Dokumentensichtung
Stufe 2 Audit	Überprüfung der wirksamen Umsetzung des Managementsystems in der Praxis	Strukturierte Interviews mit dem Management, stichpunktmäßige Überprüfung von Belegen
Abschluss	Mitteilung der Ergebnisse an das Management	Abschlussgespräch
Bericht	Zusammenfassung der Ergebnisse, Erstellung des Berichts, Mitteilung an das Management	Dokumentation

## Einleitende Anmerkungen des Auditors

Stand des Managementsystems, Methodik und Schwerpunkte des Audits

### Einleitung zum Zertifizierungsbericht der CROSSSOFT. GmbH

Der vorliegende Zertifizierungsbericht gibt einen Überblick über die Aktivitäten der CROSSSOFT. GmbH im Bereich der auditierten Managementsysteme zum Zeitpunkt dieser Stichprobe. Seit diesem Jahr betreibt CROSSSOFT. GmbH ein Qualitätsmanagementsystem nach ISO 9001:2015 sowie ein Informationssicherheitsmanagementsystem nach ISO 27001:2022. Um die Implementierung und Dokumentation dieser Managementsysteme zu unterstützen, nutzt das Unternehmen eine spezialisierte Software der Innolytics AG. Diese Software sorgt für eine klare Struktur der Dokumentation und ermöglicht den Mitarbeitenden jederzeitigen Zugriff auf die benötigten Informationen.

Das Audit bewertet die Umsetzung und Wirksamkeit des Managementsystems der CROSSSOFT. GmbH, wobei mindestens folgende Aspekte berücksichtigt werden: Die Geeignetheit des Managementsystems zur Erfüllung des Geschäftszwecks. CROSSSOFT entwickelt in den Geschäftsbereichen Medizin und Zahnmedizin professionelle Softwarelösungen für Praxen, Medizinische Versorgungszentren (MVZs), Kliniken und große Klinikverbünde. Im Industriebereich werden anspruchsvolle Softwarelösungen, insbesondere für Technik und Abrechnung im medizinischen Umfeld, entwickelt.

Unsere High-End Plattform INFINITYQ HEALTH bildet die Grundlage für zahlreiche Standardprodukte, die vom Patienten-, Ambulanz- und Stationsmanagement über Ressourcen-Disposition und komplexe Terminplanung bis hin zu anspruchsvollsten Spezialdokumentationen medizinischer Fachbereiche reichen. Dabei verbinden wir außergewöhnliche Entwicklungskompetenz und Branchenwissen, um sowohl Standardanwendungen anzupassen und zu implementieren, als auch maßgeschneiderte Speziallösungen zu entwickeln.

So wurde bereits 2010 der HL7-Enterprise Service Bus von CROSSSOFT eingeführt, um den zeitaufwendigen und fehleranfälligen Prozess der Mehrfachdatenpflege in Krankenhausinformationssystemen zu optimieren. Die Kombination dieses HL7 Kommunikationsservers mit unseren Standardanwendungen gewährleistet eine nahtlose Integration in bestehende IT-Landschaften.

Die Synergien zwischen den Geschäftsbereichen zeigen sich unter anderem in der Entwicklung von Materialwirtschaftssystemen sowie Abrechnungs- und Buchhaltungskomponenten, die auch in Kliniken als voll integrierte Lösungen oder als speziell für das Klinikpersonal gestaltetes unkompliziertes SAP-Frontend eingesetzt werden können. CROSSSOFT liefert nicht nur Produkte, sondern entwickelt mit agilen Methoden anspruchsvollste Software und begleitet seine Kunden über den kompletten Life Cycle, während gleichzeitig ein kontinuierlicher Know-how-Transfer an unsere Kunden stattfindet.

Das Audit berücksichtigt auch wichtige Nachweise zur Konformität mit den Anforderungen der relevanten Managementsystemnormen oder einer gleichwertigen Dokumentation, sowie die Überwachung, Messung, Berichterstattung und Überprüfung der Leistung anhand relevanter Ziele und Vorgaben. Des Weiteren wird die Fähigkeit und Leistung des Managementsystems hinsichtlich der Einhaltung gesetzlicher, behördlicher und vertraglicher Anforderungen sowie die Steuerung der operativen Prozesse in den Fokus genommen. Interne Audits und Managementbewertungen, die Verantwortung des Managements für die Unternehmensrichtlinien und die Zusammenhänge zwischen Normanforderungen, Richtlinien, Leistungszielen, rechtlichen Vorgaben, Verantwortlichkeiten, der Kompetenz des Personals, Betrieb, Verfahren, Leistungsdaten sowie den Ergebnissen interner Audits werden ebenfalls umfassend untersucht.

Dieser Bericht bietet somit eine detaillierte Einsicht in die aktuelle Situation und Leistungsfähigkeit der CROSSSOFT. GmbH im Kontext ihrer Managementsysteme.

## Dokumentenauswertung (Stufe 1 Audit)

Umsetzung der Anforderungen aus Kapitel 7.5 (Dokumentierte Information)

Im Rahmen des Zertifizierungsaudits wurde zunächst überprüft, ob die von CROSSSOFT GmbH angelegten Grundlagen und Ziele relevant sind. Dazu zählen unter anderem die Definition der Qualitäts- und Informationssicherheitspolitik, die Festlegung der Geltungsbereiche für das Managementsystem sowie die Kriterien zur Erfassung von Informationen, die für die Informationssicherheit von Bedeutung sind. Das Unternehmen hat sich eine kontinuierliche Verbesserung seiner Leistungen zum Ziel gesetzt, um Kundenvertrauen sowie eine hohe Zufriedenheit sowohl bei Kunden als auch bei Mitarbeitern zu fördern. Des Weiteren umfasst das Ziel die Einhaltung gesetzlicher Vorgaben und die Sicherstellung von Sicherheitsstandards durch definierte technische und organisatorische Maßnahmen.

Es wurde überprüft, inwieweit CROSSSOFT GmbH Prozesse und für die Steuerung dieser Prozesse ergänzende Dokumente angelegt hat. Dazu zählen unter anderem Richtlinien zur Kundenberatung, zur Erstellung von Angeboten, zur Umsatzoptimierung sowie zur Durchführung von Schulungsmaßnahmen. Jedes dieser Dokumente bietet klare Vorgaben und beschreibt die relevanten Schritte zur Sicherstellung der Qualität und der informationssicheren Handhabung von Daten. Des Weiteren wurden Prozessbeschreibungen erarbeitet, die den Ablauf in den jeweiligen Bereichen systematisch darlegen, um Effizienz und Qualität in der Auftragsabwicklung zu gewährleisten.

Schließlich wurde geprüft, inwieweit Risiken und Chancen aktuell sind und der Umgang angemessen. Dazu zählen unter anderem die Analyse von Informationssicherheitsrisiken bei der Nutzung von Endgeräten, Cloud-Diensten und Netzwerkinfrastrukturen sowie die Berücksichtigung rechtlicher Risiken, die aus der Nutzung von Marketingmaterialien und der Kaltakquise neuer Kunden resultieren. Die Risiken wurden identifiziert, bewertet und Schutzziele definiert, um die Informationssicherheit zu gewährleisten und das Vertrauen der Kunden zu stärken.

Zum Zeitpunkt des Zertifizierungsaudits waren die Anforderungen an die Erstellung eines ersten Systemaudits sowie einer Managementbewertung erfüllt, die Dokumente lagen vor. Dabei wurden alle relevanten Richtlinien, Prozesse und Dokumentationen erfolgreich erstellt und implementiert, um den hohen Standards der ISO 9001 und ISO 27001 zu entsprechen.

Gibt es dokumentierte Prozesse für die Softwareentwicklung gemäß ISO 9001 und ISO 27001? Überprüfen Sie, ob alle relevanten Prozesse dokumentiert sind. Dies schließt die Erstellung, Wartung und Überprüfung der Dokumentation ein.

Frage 1  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Wurden Schulungen zur Sensibilisierung für Informationssicherheit durchgeführt? Fragen Sie nach Schulungsprogrammen für Mitarbeiter zu Informationssicherheit. Überprüfen Sie, ob alle Mitarbeiter regelmäßige Schulungen erhalten.

Frage 2  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Existieren Richtlinien für das Management von Softwarefehlern? Bewerten Sie, ob es offizielle Verfahren zur Identifizierung und Behebung von Softwarefehlern gibt. Dies ist wichtig für die Qualitätssicherung.

Frage 3  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Sind die Qualitätsziele für Softwareprojekte dokumentiert? Prüfen Sie, ob klare, messbare Qualitätsziele formuliert und dokumentiert sind. Diese Ziele sollten regelmäßig überwacht werden.

Frage 4  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Gibt es ein System zur regelmäßigen Überprüfung von Sicherheitsmaßnahmen? Überprüfen Sie, ob Sicherheitsmaßnahmen regelmäßig auf ihre Wirksamkeit überprüft werden. Dies betrifft auch die Reaktion auf Sicherheitsvorfälle.

Frage 5  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Wird die Kundenzufriedenheit regelmäßig gemessen und analysiert? Fragen Sie nach Verfahren zur Erfassung der Kundenzufriedenheit. Die Analyse sollte in die Produktentwicklung einfließen.

Frage 6  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Existiert eine Risikoanalyse für Softwareprojekte? Prüfen Sie, ob eine strukturierte Risikoanalyse durchgeführt wird. Diese sollte identifizierte Risiken und entsprechende Maßnahmen umfassen.

Frage 7  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Werden Änderungen an Softwareprodukten dokumentiert und kommuniziert? Bewerten Sie den Prozess für das Änderungsmanagement. Änderungen müssen klar dokumentiert und kommuniziert werden.

Frage 8  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Gibt es eine zentrale Anlaufstelle für Sicherheitsvorfälle? Fragen Sie, ob ein Team oder eine Person für die Bearbeitung von Sicherheitsvorfällen zuständig ist. Dies ist entscheidend für die Reaktionsfähigkeit.

Frage 9  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Existiert ein Prozess zur kontinuierlichen Verbesserung? Überprüfen Sie, ob der Prozess zur kontinuierlichen Verbesserung festgelegt und dokumentiert ist. Dies sollte Feedback und Lessons Learned einbeziehen.

Frage 10  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Wird die Software regelmäßig auf Sicherheitsanfälligkeiten geprüft? Fragen Sie, ob regelmäßige Sicherheitsüberprüfungen oder Penetrationstests durchgeführt werden. Dies ist wichtig zur Sicherstellung der Softwareintegrität.

Frage 11  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Sind alle relevanten gesetzlichen Anforderungen an die Softwareentwicklung bekannt und dokumentiert? Bewerten Sie, ob alle gesetzlichen Vorgaben in Bezug auf Softwareentwicklungen berücksichtigt werden. Dies ist besonders im medizinischen Bereich wichtig.

Frage 12  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Gibt es ein Verfahren zur Verarbeitung von personenbezogenen Daten? Überprüfen Sie, ob Verfahren zur Verarbeitung und zum Schutz personenbezogener Daten existieren. Dies ist wichtig für die Einhaltung von Datenschutzbestimmungen.

Frage 13  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Ist die Dokumentation der Softwarearchitektur vollständig und aktuell? Fragen Sie nach der Vollständigkeit und Aktualität der Softwarearchitekturdokumentation. Eine klare Dokumentation ist für das Verständnis entscheidend.

Frage 14  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Existieren etablierte Kommunikationskanäle für den Know-how-Transfer zwischen den Teams? Prüfen Sie, ob strukturierte Kommunikationskanäle zur Sicherstellung des Know-how-Transfers vorhanden sind. Dies fördert die Zusammenarbeit und Effizienz.

Frage 15  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Wird die Leistung des Support-Teams regelmäßig evaluiert? Fragen Sie nach einem System zur regelmäßigen Evaluierung der Support-Team-Leistung. Dies hilft, die Kundenzufriedenheit zu steigern.

Frage 16  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Gibt es ein Prozess zur Handhabung von Kundenfeedback nach der Softwareübergabe? Überprüfen Sie, ob es Verfahren gibt, um Kundenfeedback zu sammeln und zu verwenden. Dies fördert die kontinuierliche Verbesserung der Produkte.

Frage 17  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Sind alle Mitarbeiter über ihre Rolle im Qualitätsmanagement informiert? Fragen Sie, ob alle Mitarbeiter transparent über ihre Verantwortlichkeiten im Qualitätsmanagement sind. Klarheit ist entscheidend für den Erfolg.

Frage 18  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Gibt es einen klaren Prozess zur Priorisierung von Software-Features? Überprüfen Sie, ob der Prozess zur Priorisierung von neuen Features klar definiert ist. Eine strukturierte Herangehensweise ist für die Ressourcenzuweisung wichtig.

Frage 19  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich

Wurde die ISO 9001 und ISO 27001 Zertifizierung regelmäßig auditiert? Fragen Sie nach der Historie der Audits für ISO-Zertifizierungen. Regelmäßige Audits sind für die Aufrechterhaltung von Standards entscheidend.

Frage 20  
0 / 0 Punkte

Ja

✓ Keine Korrekturmaßnahmen erforderlich