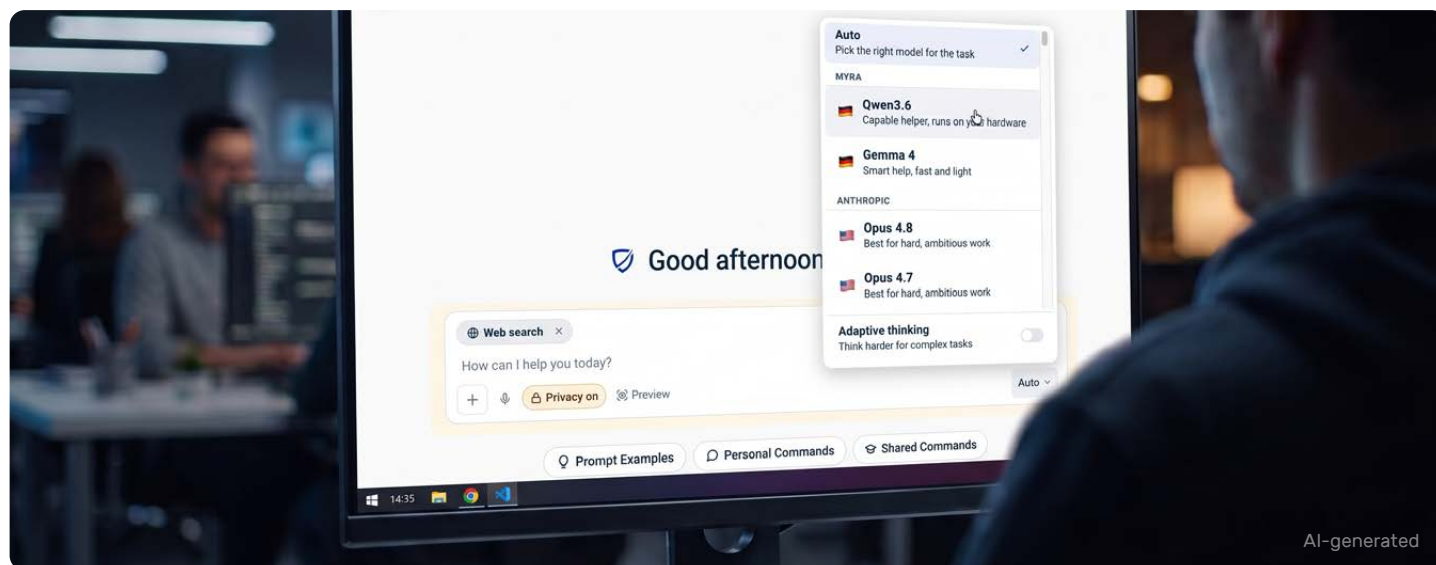




CASE STUDY – COMPLIANCE

Datensichere KI-Nutzung:

So arbeitet die Compliance-Abteilung von Myra sicher und produktiv mit KI



AI-generated

Datensichere KI-Nutzung: Wie die Compliance-Abteilung von Myra mit AI Workspace ISMS-Dokumente schneller erstellt

Executive Summary

Sicherheitsdokumentation altert schnell. Was einmal sauber formuliert war, sammelt mit der Zeit Zusätze, Ausnahmen und Wiederholungen an, die kaum noch jemand überblickt. Das Compliance-Team von Myra Security begegnet diesem Problem mit einem eigenen Agenten im AI Workspace, dem ISMS Policy Writer. Er analysiert bestehende Informationssicherheits-Richtlinien, verschlankt sie und überführt sie in eine klare, einheitliche Struktur.

Der Agent gehört zu den frühen produktiven Anwendungen des AI Workspace, das Myra entwickelte, nachdem am Markt keine Lösung die eigenen Anforderungen an Datenschutz, Sicherheit und Compliance auf KRITIS-Niveau erfüllte. Inzwischen begleitet der ISMS Policy Writer die Compliance-Fachleute täglich beim Erstellen neuer Dokumente, Schritt für Schritt in Dialogform.

Der Effizienzgewinn ist deutlich: Der Agent spart der Abteilung rund fünf Stunden pro Tag oder hochgerechnet über 120 Stunden pro Monat. Die gesamte Verarbeitung bleibt dabei in einer datenschutzkonformen Umgebung auf der eigenen Infrastruktur von Myra, und die fachliche Endkontrolle liegt weiterhin beim Menschen.

Der Agent spart der Abteilung rund fünf Stunden pro Tag oder hochgerechnet über 120 Stunden pro Monat.

Ausgangslage: gewachsene Dokumente, hoher Pflegeaufwand

Das Informationssicherheits-Managementsystem (ISMS) regulierter Organisationen besteht aus einer gestaffelten Dokumentenhierarchie: von der übergreifenden Leitlinie über themenspezifische Richtlinien und Verfahrensanweisungen bis zu Aufzeichnungen als Nachweis. Diese Dokumente müssen konsistent, verständlich und aktuell sein, denn sie sind die Grundlage für Audits, Zertifizierungen und den gelebten Sicherheitsbetrieb.

In der Praxis wächst ein ISMS über Jahre. Richtlinien werden ergänzt, überarbeitet und dupliziert. Dabei entstehen typische Probleme:

- **Aufgeblähte Dokumente:** Historisch gewachsene Richtlinien enthalten Redundanzen, veraltete Passagen und vermischte Inhaltsebenen, die eine Pflege erschweren.
- **Uneinheitliche Struktur:** Ohne konsequente Systematik driften Dokumente in Aufbau, Terminologie und Detailtiefe auseinander, was Audits verlangsamt.
- **Hoher manueller Aufwand:** Analyse, Verschlinkung und Neustrukturierung binden erfahrene Compliance-Fachleute über viele Stunden, deren Expertise an anderer Stelle in diesem Zeitraum fehlt.
- **Bindung von Expertenwissen:** Die Arbeit erfordert Fachwissen zu Normen und internen Vorgaben und lässt sich nicht ohne Weiteres delegieren.

ISMS-Dokumente beschreiben die eigenen Schutzmaßnahmen und gehören somit zu den sensiblen Daten, die nicht unkontrolliert abfließen dürfen. Ein KI-Werkzeug, das solche Informationen an intransparente Drittdienste weiterreicht, ist für regulierte Organisationen keine Option. Mit dem selbst entwickelten AI Workspace stellt Myra eine datenschutzkonforme KI-Nutzung sicher.

PRIMÄRE PROJEKTZIELE:

- Bestehende ISMS-Dokumente schneller sichten, verschlanken und neu ordnen
- Gliederung und Sprache über alle Dokumentenebenen hinweg angleichen
- Compliance-Fachleute von wiederkehrender Dokumentenarbeit befreien
- Kontrollierter Betrieb in einer KI-Umgebung, die Datenschutz und Datensicherheit gewährleistet

Technologische Umsetzung: vom Altbestand zum sauberen Zielformat

Das Compliance-Team hat den ISMS Policy Writer direkt im AI Workspace aufgesetzt und über eine Projekt- und Prompt-Konfiguration auf die interne Dokumentensystematik zugeschnitten. Passende Guardrails verhindern den Abfluss sensibler Inhalte und zielgenaue Agentenanweisungen sichern die Qualität der Ergebnisse.

Reicht eine Fachkraft eine bestehende Richtlinie zur Prüfung ein, analysiert der Agent das Dokument, entfernt Redundanzen und überführt den Inhalt in eine klare, an der ISMS-Hierarchie ausgerichtete Struktur mit konsistenter Terminologie und Formatierung. Technische Konfigurationsvorgaben und verbindliche Anforderungen

ordnet er dabei sauber der jeweils richtigen Ebene zu: als Verpflichtung in das übergeordnete Richtlinien-Dokument oder als operatives Ziel mit Prüfschritten in die zugehörige Verfahrensanweisung.

Zwei Authoring-Skills führen Nutzende dialogbasiert und Schritt für Schritt mittels Fragen durch das Erstellen neuer Dokumente.

- **ISMS Policy Authoring Skill:** begleitet die Erstellung eines neuen Richtlinien-Dokuments, entweder von Grund auf oder auf Basis eines vorhandenen Entwurfs beziehungsweise von Notizen.
- **ISMS SOP Authoring Skill:** begleitet die Erstellung einer neuen Verfahrensanweisung.

Jeder Vorgang bleibt innerhalb des AI Workspace abgesichert. Personenbezogene Daten werden automatisch maskiert, Eingaben gegen Keyword-Missbrauch und Prompt Injection geprüft, und ein DSGVO-Art.-30-konformes Audit-Log zeichnet jede Interaktion auf. So bleibt jederzeit kontrollierbar und nachvollziehbar, welche Inhalte wohin gelangen.

Bevor ein überarbeitetes oder neu erstelltes Dokument Gültigkeit erlangt, prüft eine erfahrene Fachkraft das KI-generierte Ergebnis und gibt es erst danach frei. Diese qualifizierte menschliche Endkontrolle ist dem Human-in-the-loop-Prinzip folgend bewusst fest verankert.

Mehrwerte & Chancen

Der Wert des ISMS Policy Writer bemisst sich an zwei Größen: der Zeit, die er der Compliance-Abteilung freiräumt, und der Qualität, die er in die Dokumentenlandschaft bringt. Beide Effekte greifen ineinander, denn schlankere und einheitlichere Dokumente lassen sich einfacher pflegen und prüfen. Die folgenden Punkte fassen die Ergebnisse aus dem täglichen Einsatz zusammen.

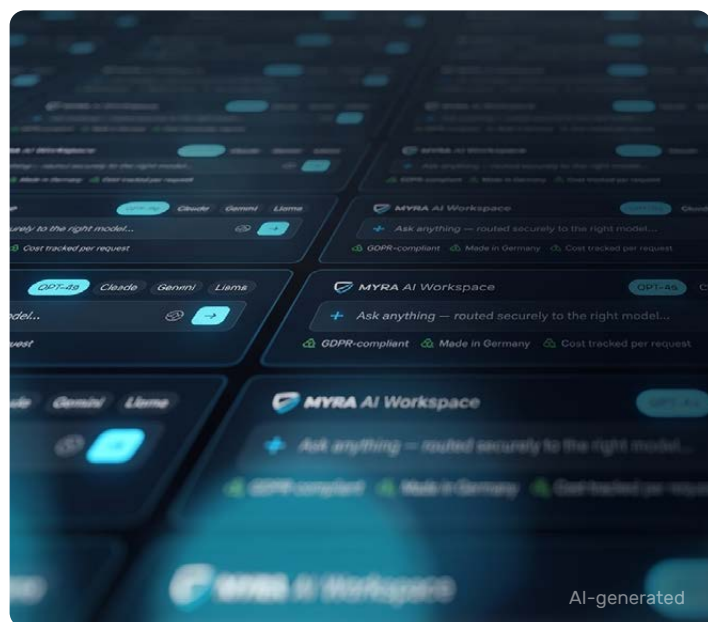
ERZIELTE MEHRWERTE:

- Zeitersparnis von rund fünf Stunden pro Tag bei täglichem Einsatz in der Compliance-Abteilung
- Konsistente Struktur und Terminologie über die gesamte ISMS-Dokumentenhierarchie hinweg
- Verschlinkte, wartbare Dokumente statt historisch gewachsener, aufgeblähter Richtlinien
- Entlastung erfahrener Compliance-Fachleute von repetitiven Aufgaben
- Schnellere Audit-Vorbereitung durch klar strukturierte, aktuelle Dokumente
- Datensichere und datenschutzkonforme KI-Umgebung auf eigener Infrastruktur

Chancen & Ausblick: vom internen Effizienz-Boost zur Kundenlösung

Der ISMS Policy Writer ist nur ein Beispiel für mögliche Einsatzszenarien des AI Workspace. Allein in der Compliance-Abteilung von Myra finden sich viele weitere Anwendungsfälle, vom KI-unterstützten Compliance Check, über einen Audit Planner bis hin zu einem Software Procurement Assessor. Über den offenen MCP-Standard lassen sich interne Wissensquellen anbinden, wobei jeder Tool-Aufruf weiterhin die Policies, Budgets und das Audit-Log des AI Workspace durchläuft.

In anderen Unternehmensbereichen wie Vertrieb, Marketing, HR/Recruiting, Legal, Finance und IT hat sich die sichere KI-Nutzung über AI Workspace ebenfalls im Betriebsalltag bewährt und für einen Effizienz-Boost gesorgt. Daher bietet Myra die Plattform auch als Kundenlösung für Organisationen mit denselben hohen Anforderungen an Datenschutz, Sicherheit und Compliance an, die generative KI nutzen und zugleich digitale Souveränität wahren wollen.



Resümee

Mit AI Workspace lässt sich das Potenzial von KI im Compliance-Bereich ohne Einschränkungen bei Datensicherheit und Datenschutz nutzen. Der im AI Workspace betriebene ISMS Policy Writer erleichtert und beschleunigt alltäglich anfallende Abläufe: Dokumente werden schneller gepflegt und neu erstellt, die Dokumentenlandschaft bleibt konsistent, und das Compliance-Team gewinnt wertvolle Zeit für anspruchsvollere Aufgaben, ohne die inhaltliche Hoheit abzugeben.

Der Anwendungsfall verdeutlicht, dass sich generative KI auch in einem hochregulierten Umfeld verantwortungsvoll und sicher einsetzen lässt. Dazu braucht es klare Regeln, transparente Abläufe sowie eine abschließende Prüfung durch den Menschen.

Der ISMS Policy Writer spart meinem Team rund fünf Stunden am Tag. Die gewonnene Zeit fließt jetzt in die fachliche Bewertung statt in das Entwirren alter Richtlinien. Das Ergebnis des sicheren KI-Einsatzes ist eine einheitliche Systematik über alle Dokumente hinweg, die uns die Audit-Vorbereitung erleichtert.“

Stefan RöB

Teamlead Compliance bei Myra Security

ZERTIFIZIERT, GEPRÜFT, IN DEUTSCHLAND BETRIEBEN

Myra ist BSI-qualifiziert für KRITIS-Betreiber und nach ISO 27001 auf Basis von IT-Grundschutz, BSI C5 Typ 2, PCI DSS sowie weiteren Standards zertifiziert. Als deutsches Unternehmen mit 100 % EU-Gesellschafterstruktur und ohne US-Mutterkonzern unterliegt Myra allein europäischer Rechtsprechung, frei von CLOUD-Act-Exposition.

ISO 27001 BSI zertifiziert
auf der Basis von IT-Grundschutz
Zertifikat Nr.: BSI-IGZ-0667-2024

PCI DSS
Certified

BSIG
KRITIS-qualifiziert



KRITIS
Nachweis gemäß
§ 8a Abs. 3 BSIG



Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach § 3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | KRITIS-Betreiber gemäß § 8a Abs. 3 BSIG | Qualitätsmanagement nach ISO 9001