IRON MOUNTAIN®

WHITE PAPER

EIN PRAKTISCHER LEITFADEN ZU EINEM RISIKOMANAGEMENTSYSTEM FÜR DAS ARCHIV- UND INFORMATIONSMANAGEMENT

BEWÄHRTE PRAKTIKEN. NEUE DENKANSÄTZE.
ALLES IN EINER RESSOURCE.

INHALTSVERZEICHNIS

WESHALB IST DIESES DOKUMENT LESENSWERT?

In der heutigen informationsorientierten Wirtschaft ist es nicht genug für Organisationen zu sagen „Wir kennen unsere Informationsrisiken." Zeitungen sind voll mit Berichten darüber, wie eine unsachgemäße Handhabung von Informationen zu Bußgeldern, Sanktionen, Rufschädigung und einem Vertrauensverlust auf Kundenseite geführt haben.

Alle Unternehmen, insbesondere diejenigen, die stark reglementiert sind, müssen proaktiv sein und eine Methode zur Risikominderung und Kontrolle entwickeln, die alle Lebenszyklusstadien der Informationen abdeckt – von der Erstellung bis zur sicheren Vernichtung der Informationen.

Die Menge der Informationen wächst weiterhin exponentiell, was die Kontrolle und Handhabung immer mehr erschwert. Dadurch wird die Notwendigkeit eines Risikomanagements zur gezielten Handhabung der Risiken des Informationsmanagements schnell offensichtlich. Dieser Rahmenplan ist eine unerlässliche Komponente eines Information-Governance-Programms.

Sicherzustellen, dass Informationsrisiken gut verstanden, dokumentiert und dann kontrolliert werden, um sie zu mindern, sind Praktiken, denen jedes Unternehmen nachgehen sollte. Angesichts externer Bedrohungen wird dies auch von unseren Aufsichtsbehörden erwartet.

In diesem Dokument finden Sie hilfreiche Ratschläge zu Kontrollen, die zur effektiven Handhabung informationsbezogener Risiken aufgestellt werden müssen, sowie einen Vorschlag für ein Risikobewertungssystem zur Erfassung des aktuellen Zustandes des Kontrollumfelds Ihres Unternehmens.

INFORMATION GOVERNANCE

Information Governance ist ein multidisziplinärer Rahmen zur Unternehmensverantwortlichkeit, der das richtige Verhalten bei der Bewertung von Informationen sowie die Definition der Rollen, Richtlinien, Prozesse und Messgrößen sicherstellt, die für das Management des Lebenszyklus der Informationen notwendig sind, einschließlich der rechtlich durchsetzbaren Vernichtung.

EINFÜHRUNG

Mitglieder des Customer Advisory Board (CAB) von Iron Mountain haben Anfang 2014 einen Ausschuss gebildet, um bewährte Praktiken zum Thema Archiv- und Informationsmanagementrisiko zu identifizieren und zu teilen. Dabei gingen wir von der folgenden Frage aus: „Was ist die beste Möglichkeit, eine Richtlinie zum Archiv- und Informationsmanagement aufzubauen, zu unterstützen und zu überwachen?“

Durch unsere Gespräche haben wir festgestellt, dass jedes Unternehmen zwar selbst entscheidet und definiert, wie die Compliance überwacht wird, um den speziellen Anforderungen und der Kultur des Unternehmens gerecht zu werden, es aber auch bestimmte universelle Risiko- und Kontrollelemente für das Archiv- und Informationsmanagement gibt. Diese Erkenntnis veranlasste den Ausschuss dazu, diesen praktischen Leitfaden zum Risikomanagement für das Archiv- und Informationsmanagement mit dem Ziel anzulegen, eine Reihe von allgemeinen Risikokontrollen aufzustellen, die innerhalb eines Unternehmens während der fortwährenden Schaffung und Weiterentwicklung eines robusten Information-Governance-Programms mit Kollegen geteilt werden können.

METHODIK

Zu Beginn unserer Zusammenarbeit wurden die folgenden Themen vom Ausschuss als wesentlich für die Befürwortung und Entwicklung des Rahmenplans ausgewählt:

- Definition eines Risikorahmens für das Archiv- und Informationsmanagement
- Haupttreiber für Compliance
- Identifikation von wichtigen Kontrollen für das Archiv- und Informationsmanagement
- Institutionalisierung
- Rollen und Verantwortlichkeiten
- Erfolgsmessung
- Aktionsplan zur Verbesserung

Dieser Leitfaden zur Entwicklung und Erhaltung eines Risikomanagementsystems für das Archiv- und Informationsmanagement dient zur Verwendung in unternehmensinternen Compliance-und Information-Governance-Programmen. Dieser Rahmenplan ist keineswegs definitiv oder abschließend. Er ist vielmehr der erste Schritt in der Entwicklung von Klarheit und Orientierung dazu, wie eine ordnungsgemäße Compliance hinsichtlich von Informationen geschaffen werden kann. Wir hoffen, dass Sie diesen Leitfaden zu Beginn eines internen Dialogs einsetzen, um die Unterstützung funktionsübergreifender Führungskräfte hinsichtlich Ihrer Compliance-Anforderungen und Plattform zu gewinnen.

RISIKOMANAGEMENTSYSTEM FÜR DAS ARCHIV- UND INFORMATIONSMANAGEMENT

Das Risikomanagement für das Archiv- und Informationsmanagement stellt ein betriebliches Selbstbeurteilungsprogramm auf, mit dem Führungskräfte ihre eigenen Leistungen hinsichtlich einer Reihe von vorgegebenen Kontrollen bewerten können. Ein solches Programm bietet Führungskräften ein umfassendes und einheitliches Protokoll unabhängig von ihrem Standort oder der Art der ausgeführten Arbeit, um potenzielle Schwachstellen im Aufbau oder der Umsetzung der internen Archiv- und Informationsmanagementprozesse zu identifizieren und zu beheben.

Durch einen Selbstbeurteilungsprozess können Geschäftsbereiche Probleme identifizieren und die Einführung von Korrekturmaßnahmen vorantreiben, um wesentliche betriebliche, rechtliche, Compliance-bezogene und rufschädigende Risiken und Kosten zu vermeiden, zu beheben oder zu mindern. Dieser Prozess wird durch Hauptfunktionsbereiche wie Archiv- und Informationsmanagement, Compliance, IT, Informationssicherheit und Datenschutz sowie Internen Audit unterstützt, um Beiträge zur Erstellung des Programms zu liefern. Er hilft zudem auch bei der Umsetzung und unterstützt die Erstellung und Durchführung eines Korrekturplans, nachdem die Beurteilungen stattgefunden haben.

Alle mit dem Lebenszyklus der Informationen verbundenen Risiken müssen im Zusammenhang mit Richtlinien, Verfahren, Branchenstandards und bewährten Praktiken verwaltet werden, um sicherzustellen, dass behördliche, betriebliche, Compliance-bezogene und rechtliche Anforderungen erfüllt werden.

Das Risikomanagementsystem für das Archiv- und Informationsmanagement sollte als Bestandteil einer breiteren Palette von unternehmensweiten Compliance-Kontrollen positioniert werden. Unternehmens-Compliance wird beschrieben als „konkrete Bemühungen eines Unternehmens zur Vermeidung, Erkennung und anderweitigen angemessenen Reaktion auf unrechtmäßiges Verhalten verbunden mit den Handlungen der Personen, die im Namen des Unternehmens tätig sind. Das bezieht sich auf Direktoren, leitende Angestellte, Mitarbeiter, Vertreter und unabhängige Auftragnehmer.“[1]

Eine Reihe von Standardkontrollen für die Geschäftstätigkeit muss für ein Unternehmen durch eine interne Governance-Stelle aufgestellt werden. Auch wenn nicht alle Kontrollen auf alle Geschäftsbereiche zutreffen, die Risikokontrollen für das Archiv- und Informationsmanagement müssen für alle Funktionen (z. B. Personalabteilung oder Rechts-/Compliance-Abteilung) und alle Standorte (z. B. Nordamerika oder Asien) zwingend vorgeschrieben sein.

HAUPTTREIBER

Die überzeugenden Gründe für das Aufstellen eines Risikomanagementsystems für das Archiv- und Informationsmanagement sind in einigen Fällen universell und in anderen Fällen spezifisch für eine Region oder individuelle Gerichtsbarkeit.

Generell bedeutet ein Haupttreiber die Fähigkeit, Nachweis für ordnungsgemäße Risikomanagement- und Compliance-Protokolle für Behörden, Kunden und Wirtschaftsprüfer zu erbringen. Allerdings ging aus dem **2013|2014 Cohasset/ARMA Information Governance Benchmark Bericht** hervor, dass nur 8 % der Unternehmen irgendeine Form von Messgrößen zur Verfolgung der Archiv- und Informationsmanagementaktivitäten einsetzen und magere 17 % Compliance-Audits zum Archiv- und Informationsmanagement durchführen. Zusätzlich zu diesen niedrigen Zahlen gaben nur 7 % der Umfrageteilnehmer an, dass ihre Mitarbeiter in die Archiv- und Informationsmanagementprogramme einbezogen werden[1].

Beispiele für Haupttreiber sind allgemeine und branchenspezifische Compliance-Vorschriften und Datenschutzverpflichtungen. In den USA gelten der Dodd-Frank Act, der Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), der Federal Information Security Management Act (FISMA) und der Sarbanes-Oxley Act (SOX). Beispiele für die EU sind die Financial Conduct Authority (FCA) und die Prudential Regulatory Authority (PRA). Die **Europäische Datenschutz-Grundverordnung (EU-DS-GVO)**, die die

[1] http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/C/Compliance-Benchmark-Report.aspx

Datenschutzrichtlinie von 1995 (EU Directive 95/46/EC) ersetzen soll, ist eine weitere starke Motivation für die Einführung des Risikomanagementsystems für das Archiv- und Informationsmanagement[2].

Angesichts der Vielzahl von Treibern und unserer derzeitigen Unfähigkeit, die Einhaltung der Richtlinien zur Minderung dieses Risikos zu verfolgen oder zu messen, besteht eine enorme zu schließende Kluft zwischen der Verpflichtung eines Unternehmens, die Informationen zu verwalten, und dem Nachweis der tatsächlichen Praxis. Es ist unrealistisch, von einem ressourcenbeschränkten Archiv- und Informationsmanagement-Personal zu erwarten, das gesamte Unternehmen zu beaufsichtigen, insbesondere wenn der Umfang und die Vielzahl elektronischer Daten beim Informationsmanagement mit berücksichtigt werden. Aus diesem Grund muss eine neue Methode entwickelt und eingeführt werden, welche die zuständigen Geschäftsbereiche für Erstellung, Empfang, Bearbeitung und Vernichtung von Informationen, miteinbezieht. Der Nachweis über die Einhaltung von Kontrollen wird das Compliance-Profil eines Unternehmens stärken und je nach Bedarf zu Risikominimierungs- und/oder Korrekturplänen für das Informationsmanagement führen.

Nur 8 % der Unternehmen verwenden Messgrößen zur „Überprüfung ihrer Erwartungen“ und nur 17 % führen Compliance-Audits zum Archiv- und Informationsmanagement durch.

Nur 7 % geben an, dass Mitarbeiter in das Archiv- und Informationsmanagement einbezogen werden.

RISIKOKONTROLLEN FÜR DAS ARCHIV- UND INFORMATIONSMANAGEMENT

In diesem Leitfaden werden neun Hauptkategorien der Risikokontrollen für das Archiv- und Informationsmanagement beschrieben, die für die Verwaltung der Informationen während ihres gesamten Lebenszyklus gelten. Diese sind:

- Governance
- Bestandsaufnahme
- Aufbewahrung
- Vernichtung
- Rechtliche Sperrfristen
- Datenschutz und Informationssicherheit
- Partnermanagement
- Personal
- Schulung

Für jede Kategorie geben wir eine kurze Beschreibung gefolgt von einer Tabelle. Die Tabelle besteht aus vier Elementen:

Kontrolle: Ein Standard der Leistung innerhalb der Kategorie, die als unerlässlich für den Risikobeurteilungsprozess in Bezug auf das Archiv- und Informationsmanagement eingestuft wurde.

Beschreibung: Eine Erklärung der Bedeutung und Relevanz der Kontrolle.

Unterstützende Informationen: Zusätzliche Anleitung zu speziellen Maßnahmen zur mit der Kontrolle verbundenen Bewertung.

Bewertung: Anleitung zur Zuordnung eines Beurteilungsergebnisses für die Kontrolle, das zur Bestimmung des Compliance-Grads eines Geschäftsbereichs verwendet wird. Es wird erwartet, dass die Teilnehmer eines Geschäftsbereichs eine Zahl von eins bis vier auswählen, basierend auf der tatsächlichen Einhaltung der Kontrolle (wobei eins der niedrigste Grad und vier der höchste ist). Beachten Sie, dass nicht alle Geschäftsbereiche die höchste Bewertung für alle Kontrollen erreichen müssen.

GOVERNANCE

Governance ist die übergreifende Management- und Verantwortlichkeitsstruktur für eine konforme Archiv- und Informationsmanagementfunktion. Auch wenn diese Kontrollen für alle Geschäftsbereiche oder auf Unternehmensebene relevant sein können, werden sie hier speziell für die Governance von Archiv- und Informationsmanagement-Funktionen dargestellt.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Überprüfung und Aufsicht durch Abteilungsleitung	Die Abteilungsleitung der Archiv- und Informationsmanagementfunktion ist aktiv involviert und für den täglichen Ablauf der Archiv- und Informationsmanagementaktivitäten verantwortlich. Es existieren Aufsichtsausschüsse für das Risikomanagement, um den Status des Archiv- und Informationsmanagementprogramms zu überwachen (z. B. Information Governance Council, Informationsrisikoausschüsse). Bedeutende betriebliche Probleme, Bedenken hinsichtlich des Geschäftsprozesses, der Risikokapazität und der Infrastruktur, und rechtliche, Compliance-bezogene und behördliche Kontrollanliegen werden rechtzeitig überprüft, dokumentiert und bearbeitet.	– Das Information Governance Council oder die entsprechende Versammlung wird regelmäßig einberufen. – Teilnehmer sind Vertreter aller relevanten Bereiche, z. B. Seniormanagement des Archiv- und Informationsmanagements, Risikomanagement, Rechtsabteilung, Compliance-Abteilung, Informationssicherheit, QM usw. – Die Tagesordnung und das Sitzungsprotokoll werden zeitnah als Nachweis der Sitzungsteilnahme und getroffenen Entscheidungen erstellt. – Folgeaktivitäten werden dokumentiert und in nachfolgenden Sitzungen angesprochen. – Bedeutende Bedenken hinsichtlich Verantwortlichkeiten und Kontrollen werden entsprechend überprüft und eskaliert.	1. Es existiert kein spezieller Ausschuss für das Archiv- und Informationsmanagement. 2. Es existieren eingeschränkte Ausschüsse mit beschränkter Mitgliedschaft. Sitzungen finden nur unregelmäßig statt, und während sich Handlungen wiederholen, erfolgt nur ein eingeschränkter Nachweis in Begleitunterlagen darüber. 3. Ein Aufsichtsausschuss mit Teilnahme der Geschäftsleitung existiert, kann aber keine Verantwortlichkeit und Entscheidungen durch dokumentierte Handlungen nachweisen. 4. Ein Aufsichtsausschuss zum Archiv- und Informationsmanagement mit Teilnahme und Unterstützung der Geschäftsleitung existiert. Klare Ziele werden aufgestellt und übermittelt. Entscheidungen und zugewiesene Verantwortlichkeiten werden dokumentiert und überwacht.
Richtlinien- und Verfahrensmanagement	Die Richtlinien zum Archiv- und Informationsmanagement werden in Übereinstimmung mit dem Richtlinienverwaltungsprozess des Unternehmens erstellt und verwaltet. Standardisierte Arbeitsabläufe für das Archiv- und Informationsmanagement stellen die Funktionen und Kontrollen eindeutig dar, die durchgeführt und nachgewiesen werden müssen, wenn Parteien mit dem Archiv- und Informationsmanagementprozess interagieren.	– Die Verwaltung der Richtlinien und Verfahren zum Archiv- und Informationsmanagement muss von einer bestimmten oberen Führungskraft/einem bestimmten Team aus Führungskräften unterstützt werden, die für den Inhalt der Richtlinien und unterstützenden Verfahren zuständig ist/sind. – Geplante Prüfungen und Aktualisierungen werden innerhalb eines dokumentierten Verfahrens durchgeführt, um Richtlinien zu genehmigen, zu ändern, zu ersetzen und außer Kraft zu setzen. – Es existiert eine Bestandsliste aller Richtlinien, die vom Archiv- und Informationsmanagement verwaltet werden, und öffentliche Versionen der Richtlinien werden gemäß dem Aufbewahrungsplan für Archivbestände archiviert. – Der Nachweis einer ordnungsgemäßen Richtlinienverwaltung umfasst Versionskontrolle, Sitzungsprotokolle, Dokumentation von Änderungsgenehmigungen und außer Kraft gesetzten oder ersetzten Richtlinien. – Verfahren werden in angemessener Regelmäßigkeit überprüft, um sicherzustellen, dass Anweisungen korrekt und aktuell sind.	1. Es existieren keine formellen Richtlinien und Verfahren zum Archiv- und Informationsmanagement. 2. Es existieren Richtlinien und Verfahren zum Archiv- und Informationsmanagement, diese werden aber nicht regelmäßig aktualisiert oder von der zuständigen Instanz genehmigt oder sie sind unvollständig. Es gibt keine formelle und einheitliche Methode zur Dokumentation und Kommunikation von Aktualisierungen. 3. Die Richtlinien und Verfahren zum Archiv- und Informationsmanagement werden regelmäßig aktualisiert und an die relevanten Parteien weitergeleitet, aber ersetzte und ungültige Versionen werden nicht ordnungsgemäß aktualisiert. 4. Die Richtlinien und Verfahren zum Archiv- und Informationsmanagement werden auf dem neusten Stand gehalten, von den zuständigen Instanzen genehmigt und den wichtigsten Entscheidungsträgern und betroffenen Abteilungen und Mitarbeitern zur Verfügung gestellt. Ersetzte und ungültige Versionen werden archiviert und gemäß dem Aufbewahrungsplan für Archivbestände aufbewahrt.

[2] http://www.ironmountain.de/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/P/Prepare-Now-For-the-New-EU-Data-Protection-Law.aspx

Rechtlicher/behördlicher Änderungsmanagement-Prozess	Neue/aktualisierte Vorschriften und Gesetze werden auf ihre Anwendbarkeit auf das Archiv- und Informationsmanagementprogramm überwacht, insbesondere diejenigen, die Auswirkungen auf Aufbewahrungsfristen haben. Das Management der Rechtsabteilung, Compliance-Abteilung, des Archiv- und Informationsmanagements, der Geschäftsbereiche (und andere, wie Drittparteien, je nach Art der Angelegenheit) sind involviert, um die Auswirkungen auf das Geschäft zu beurteilen. Richtlinien, Verfahren und Aufbewahrungspläne für Archivbestände werden zeitnah bewertet und geändert. Personalschulungen werden nach Bedarf aufgefrischt.	– Die Teams von Rechtsabteilung, Compliance und/oder Archiv- und Informationsmanagement haben einen bestehenden Prozess zum Erhalt von Informationen hinsichtlich anstehender oder angekündigter rechtlicher oder behördlicher Änderungen, die Auswirkungen auf das Archiv- und Informationsmanagementprogramm haben würden.	1. Es gibt keinen formellen Prozess zur Identifikation, Korrektur oder Bekanntmachung von Änderungen an Vorschriften und Gesetzen, die Auswirkungen auf das Archiv- und Informationsmanagementprogramm haben. 2. Rechtliche und behördliche Änderungen, die Auswirkungen auf das Archiv- und Informationsmanagementprogramm haben, werden für den Einzelfall identifiziert, und die Verbreitung der Anforderungen findet unregelmäßig statt. 3. Rechtliche und Compliance-Teams überprüfen Änderungen regelmäßig, aber informieren Archiv- und Informationsmanagement nicht konsequent über alle Änderungen, die Auswirkungen auf die Archiv- und Informationsmangementabläufe haben. 4. Es existiert ein formeller Prozess für die Identifikation und Überprüfung von Änderungen an rechtlichen und behördlichen Anforderungen, die Auswirkungen auf das Archiv- und Informationsmanagementprogramm haben.
Governance von Archiv- und Informationsmanagement-Tools	Die vom Archiv- und Informationsmanagement-Team verwendeten Tools (z. B. für Bestandsverfolgung) oder die von den Geschäftsbereichen verwendeten Tools für die Verwaltung der Archiv- und Informationsmanagementrichtlinien (z. B. für elektronisches Datenmanagement) werden in Übereinstimmung mit allen IT-Governance-Protokollen genehmigt. Alle Archiv- und Informationsmanagement-Tools werden ordnungsgemäß im Anwendungstool für die Bestandsaufnahme identifiziert und erfasst (siehe Bestandskontrollen). Diese Archiv- und Informationsmanagement-Tools müssen risikoklassifiziert sein und fortlaufenden Beurteilungen unterliegen, um ihr Design zu überprüfen und zu bestätigen, dass sie die angegebene Funktionalität und ihren Zweck erfüllen.	– Alle im Archiv- und Informationsmanagementprozess verwendeten Tools müssen den unternehmensweiten Richtlinien und Standards entsprechen, damit das Risiko eines Datenverlusts, unbefugten Zugriffs oder unkontrollierter Änderungen minimiert werden kann. – Die Archiv- und Informationsmanagement-Tools müssen ordnungsgemäß überwacht und kontrolliert werden, um das Archiv- und Informationsmanagement und die Aktivitäten der Geschäftseinheiten angemessen unterstützen sowie das Risiko für das Unternehmen reduzieren zu können.	1. Die Archiv- und Informationsmanagement-Tools entsprechen nicht den IT-Standards oder es finden keine regelmäßigen Überprüfungen oder Risikobewertungen statt. Die Tools sind nicht in der Anwendungsübersicht enthalten. 2. Das Archiv- und Informationsmanagementprogramm hat einige Bewertungen, entspricht aber nicht den Richtlinien oder IT-Standards. 3. Einige der Tools für das Archiv- und Informationsmangementprogramm haben keine Risikobewertung oder entsprechen nur teilweise den IT-Standards. 4. Das Archiv- und Informationsmanagementprogramm überprüft seine Tools regelmäßig auf Übereinstimmung mit unternehmensweiten IT-Kriterien und stellt sicher, dass sie in der Anwendungsübersicht des Unternehmens enthalten sind. Die Tools werden nach Risikoart klassifiziert.

BESTANDSAUFNAHME

Die Fähigkeit eines Unternehmens zu wissen, welche Daten im gesamten Unternehmen existieren sowie in welchem Format und wo diese aufbewahrt werden, zeigt sich in einer Bestandsaufnahme.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Physische Akten: Bestandsverfolgung	Physische Archivbestände an allen Standorten, vor Ort und extern, an denen das Unternehmen tätig ist, müssen inventarisiert werden. Eine zentrale Bestandsliste gewährleistet Überblick und Kontrolle der physischen Akten.	– Bestandsverfolgung für physische Akten erfasst und meldet die folgenden Daten für Kartons und/oder Akten: Bezeichnung des externen Archivanbieters oder internen Archivbereichs, Standort, Abteilung, Anzahl der Kartons/Akten, Eignung zur Vernichtung, gültige/ungültige Archivcodes, rechtlichen oder sonstigen Sperrfristen unterliegende Kartons/Akten, für Vernichtung überfällige Kartons/Akten, Kartons/Akten mit fehlenden identifizierenden Daten, zurückgeforderte und nicht nach 90 Tagen zurückgesendete Kartons/Akten.	1. Es findet keine Verfolgung des physischen Archivbestands statt. 2. Es findet keine zentrale Bestandsaufnahme für physische Akten statt. Eine Bestandsverfolgung für mehrere Archivstandorte und ggf. ausgelagerter Archive findet statt, wird aber größtenteils von unterschiedlichen Systemen und Parametern bestimmt. 3. Die physische Bestandsliste enthält die meisten empfohlenen Daten, befindet sich aber eventuell nicht in einer zentralisierten Datenbank. Mehrere Bestandslisten müssen zusammengeführt werden, um eine einheitliche Ansicht des gesamten Bestands zu generieren. 4. Die physische Archivbestandsliste ist umfassend (alle Archivstandorte sind enthalten) und sie enthält alle empfohlenen Daten. Sie wird in einer zentralisierten Datenbank gespeichert, die leicht durchsucht werden kann.
Digitale Daten: Bestandsliste/ Datenübersicht	Eine vollständige und korrekte Bestandsaufnahme aller Unternehmensanwendungen und eine umfassende Datenübersicht sind für die Verwaltung elektronischer Daten unerlässlich. Eine derartige Bestandsliste muss strukturierte, teilweise strukturierte und unstrukturierte Archivbestände umfassen, in denen sich Daten befinden könnten. Um effektiv zu sein, muss sie auf dem neusten Stand gehalten werden.	– Die Datenübersicht enthält alle elektronisch gespeicherten Informationen. – Die begleitende Anwendungsübersicht enthält alle Anwendungen, Systeme und Archivbestände innerhalb des gesamten Unternehmens. – Eine regelmäßige Pflege wird durchgeführt, um die Richtigkeit der Bestandsliste und Übersicht zu gewährleisten.	1. Es existiert keine Anwendungs- oder Datenübersicht. 2. Um eine vollständige Ansicht aller Anwendungen zu erhalten, muss auf mehrere Quellen zugegriffen werden. Die Datenübersicht ist unvollständig/enthält nicht alle elektronisch gespeicherten Informationen. 3. Eine Bestandsliste aller Anwendungen existiert, aber sie ist nicht korrekt und/oder wird nicht regelmäßig aktualisiert. 4. Eine vollständige und korrekte Bestandsliste aller Unternehmensanwendungen existiert, und eine Datenübersicht enthält alle vorhandenen elektronisch gespeicherten Informationen. Sie wird regelmäßig und planmäßig aktualisiert.

Archivbestandsindexierung durch Geschäftsbereiche	Unter Anleitung des Archiv- und Informationsmanagement-Teams muss jeder Geschäftsbereich einen ausreichend detaillierten Archivbestandsindex erstellen, um alle Prozesse hinsichtlich rechtlicher Sperrfristen, eDiscovery, eDisclosure und Abruf von Papierakten und elektronischer Inhalte zu unterstützen. Diese Indexierung umfasst die entsprechende Klassifizierung und den Lagerort für jeden identifizierten Archivbestand.	– Die Indexierung durch die Geschäftsbereiche zeigt die Verwendung des entsprechenden Archivcodes/der Archivklasse aus dem Aufbewahrungsplan des Unternehmens. – Die Indexierung beinhaltet ausreichende Informationen, damit Archivbestände schnell abgerufen werden können, wenn sie benötigt werden, rechtliche Sperrfristen für Akten verhängt werden können, oder eDiscovery/eDisclosure-Anfragen nachgekommen werden kann.	1. Geschäftsbereiche unterhalten keinen Index zusätzlich zu den Bestandslisten von externen Archivanbietern und/oder Datenübersichten. 2. Geschäftsbereiche unterhalten eine Art von Index, der aber nicht alle elektronischen und physischen Archivbestände erfasst. Er kann sich größtenteils auf physische Archivbestände konzentrieren und entspricht nicht den Anforderungen der aktuellen Aufbewahrungspläne für Archivbestände. 3. Geschäftsbereiche unterhalten einen Index zu den Archivbeständen, der allerdings nicht ganz vollständig oder korrekt ist oder nicht regelmäßig aktualisiert wird, um Änderungen der Aufbewahrungspläne des Unternehmens zu reflektieren. 4. Geschäftsbereiche unterhalten einen vollständigen und korrekten Index für alle physischen und elektronischen Archivbestände und können auf Mitteilungen zu rechtlichen Sperrfristen oder Anforderungen von Produktinformationen rechtzeitig und effektiv reagieren. Geschäftsbereiche führen mindestens jährliche Selbstkontrollen durch, um Bestandslisten von externen Archivdienstleistern mit Bestandslisten der Geschäftsbereiche in Einklang zu bringen. Änderungen der Aufbewahrungspläne für Archivbestände werden entsprechend aktualisiert.

AUFBEWAHRUNG

Aufbewahrung ist die grundlegende Voraussetzung für die Verwaltung von Archivbeständen in jedem beliebigen Format und gemäß den Gesetzen, Vorschriften und betrieblichen Verpflichtungen. Das beinhaltet die Klassifizierung von Archivbeständen, um eine Zuweisung von Aufbewahrungsregeln zu ermöglichen.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Aufbewahrungsplan für Archivbestände	Ein Aufbewahrungsplan für Archivbestände unterstützt eine konforme Verwaltung und Klassifikation von Archivbeständen in allen Formaten, Geschäftsbereichen und Rechtsordnungen. Der Plan basiert auf Gesetzen und Regeln sowie betrieblichen Anforderungen, um die Aufbewahrungsdauer für Archivbestände festzulegen. Er wird veröffentlicht und Mitarbeitern leicht zugänglich gemacht.	– Ein zentraler, unternehmensweiter, rechtlich durchsetzbarer Aufbewahrungsplan für Archivbestände wird erstellt und unterhalten. Er basiert auf Rechtsforschung, subjektiven Ansichten von juristischem oder anderweitig befugtem Personal und betrieblich ersetzten Vorschriften. – Die Aufbewahrungsfrist für jede Archivbestandsklasse wird auf eine Weise dokumentiert und gespeichert, dass sie abgerufen und überprüft werden kann. – Die Rechtsforschung wird für jeden Bereich regelmäßig aktualisiert und überprüft. – Es existiert ein Prozess zur Handhabung von rechtlichen oder behördlichen Änderungen, die Auswirkungen auf den Aufbewahrungsplan haben könnten. – Änderungen des Plans müssen allen Interessenvertretern mitgeteilt werden. – Eine lückenlos dokumentierte Historie existiert für alle Änderungen des Aufbewahrungsplans.	1. Es existiert kein Plan, um die Klassifikation von Archivbeständen oder Aufbewahrungsregeln zu dokumentieren. 2. Das Unternehmen hat mehrere von Geschäftsbereichen erstellte Pläne (keine unternehmensweite Version), die regelmäßig aktualisiert werden. 3. Unternehmensweite Aufbewahrungspläne für Archivbestände wurden für alle Bereiche entwickelt, und diese werden regelmäßig (nicht geplant oder innerhalb eines Jahres) oder unregelmäßig überprüft und aktualisiert und für Interessenvertreter veröffentlicht. 4. Unternehmensweite Aufbewahrungspläne für Archivbestände wurden für alle Bereiche entwickelt, und diese werden regelmäßig zu einem geplanten Zeitpunkt (mindestens einmal pro Jahr) überprüft und aktualisiert und für Interessenvertreter veröffentlicht.
Geplante Überprüfung/ Archivierung	Es muss eine regelmäßige Überprüfung von physischen und elektronischen Archivbeständen stattfinden, um die Lebenszyklusphase und angemessene Aufbewahrung sicherzustellen: Löschung/ Vernichtung, Archivierung, externe Lagerung usw. Diese regelmäßige Überprüfung basiert auf dem Aufbewahrungsplan für Archivbestände, um Geschäftsunterlagen und Aufbewahrungsdauer zu identifizieren. Die Überprüfung muss mindestens jährlich stattfinden.	– Jeder Geschäftsbereich führt geplante Überprüfungen/Archivierungen durch. – Inaktive Bestände werden archiviert und Bestände mit keinem fortwährenden geschäftlichen oder rechtlichen Wert, die die festgelegte Aufbewahrungsfrist erreicht haben, werden vernichtet. – Alle Mitarbeiter, die Archivbestände aufbewahren oder verwalten, müssen teilnehmen, und schriftliche Anweisungen zur Lagerung, Erhaltung oder Vernichtung von Archivbeständen werden für Papierakten und elektronische Inhalte bereitgestellt. – Mitarbeiter bestätigen, dass sie eine Überprüfung ihrer Papierakten oder elektronischen Archivbestände durchgeführt und die Anweisungen zur Lagerung, Erhaltung oder Vernichtung ihrer Archivbestände befolgt haben.	1. Obwohl die regelmäßige Überprüfung in der Archiv- und Informationsmanagementrichtlinie enthalten ist, findet keine Überprüfung oder Archivierung von Archivbeständen statt. 2. Die regelmäßige Überprüfung von Papierakten oder elektronischen Archivbeständen findet mit wahllosen und unregelmäßigen Maßnahmen statt. 3. Die geplante Überprüfung von Papierakten findet mit notwendigen Maßnahmen statt. Keine Überprüfung von elektronischen Archivbeständen. Bestätigungen von Mitarbeitern werden systematisch dokumentiert und erfasst. 4. Es findet eine geplante Überprüfung und Archivierung von Papierakten und elektronischen Archivbeständen statt, und angemessene Maßnahmen werden ergriffen. Bestätigungen von Mitarbeitern werden systematisch dokumentiert und erfasst.

Überprüfung von Backup-Medien	Geplante Überprüfungen von Backup-Medien (eine Kopie von Daten, die zum Zweck der Wiederherstellung im Fall eines Datenverlusts aufbewahrt wird) werden vorgenommen, um sicherzustellen, dass keine Kopien von Archivbeständen länger als der offizielle Archivbestand aufbewahrt werden.	– Das Archiv- und Informationsmanagementprogramm erstellt Richtlinien und Überwachungsmaßnahmen, um sicherzustellen, dass Backup-Medien erstellt und nur zum Zweck der Notfallwiederherstellung verwendet werden. – Backup-Medien werden nur dann als Archivbestandsspeicher verwendet oder selber archiviert, wenn dies von einer zuständigen Abteilung (Archiv- und Informationsmanagement, Rechtsabteilung, Compliance-Abteilung) genehmigt wurde.	1. Backup-Medien werden nicht überprüft oder vernichtet. 2. Offizielle Versionen von Archivbeständen werden nicht regelmäßig mit Backup-Kopien abgeglichen. 3. Es existiert eine Richtlinie zur Definition der ordnungsgemäßen Nutzung von Backup-Medien zur Notfallwiederherstellung. Es werden keine Maßnahmen ergriffen, um die doppelte Lagerung von Archivbeständen zu vermeiden. 4. Es existiert eine Richtlinie zur Definition der Nutzung von Backup-Medien zur Notfallwiederherstellung, nicht als Archiv, außer wenn autorisiert. Es existiert ein Prozess zur Synchronisierung der Verwaltung und Überwachung des offiziellen Archivbestands mit Kopien auf Backup-Medien.

VERNICHTUNG

Vernichtung bezieht sich auf die Entscheidung zu einem Archivbestand, der gemäß dem formellen Aufbewahrungsplan für Archivbestände des Unternehmens das Ende seiner vorgeschriebenen Aufbewahrungsdauer erreicht hat. Ein Archivbestand kann vernichtet oder zur langfristigen Archivierung übertragen werden.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Sichere Vernichtung geeigneter Archivbestände	Archivbestände, die zur Vernichtung geeignet sind, werden sicher in Übereinstimmung mit der Archiv- und Informationsmanagementrichtlinie und Informationssicherheitsprotokollen entsorgt.	– Rollen und Verantwortlichkeiten des sicheren Vernichtungsprozesses sind klar definiert und in Richtlinien und Verfahren bekannt gemacht. – Sichere Vernichtungsstandards für elektronische Daten oder physische Archivbestände werden konsequent eingehalten und überprüft.	1. Archivbestände werden nicht auf sichere Weise entsorgt. 2. Einige, aber nicht alle, geeigneten Archivbestände werden sicher vernichtet oder es gibt keine schriftliche Bestätigung der sicheren Vernichtung. 3. Geeignete Archivbestände werden sicher vernichtet, aber der Prozess wird nicht dokumentiert oder es haben sich Unstimmigkeiten im Prozess gezeigt. 4. Alle geeigneten Archivbestände werden routinemäßig und sicher entsorgt. Der Prozess wird dokumentiert und regelmäßig überprüft.
Aussetzung der Vernichtung	Die Vernichtung von Archivbeständen, die einer rechtlichen oder behördlichen Sperrfrist unterliegen, wird während der Sperrfrist ausgesetzt. Archivbestände, die während der aktiven Sperrfrist zur Vernichtung in Frage kommen, können nicht vernichtet werden, bis die Sperrfrist aufgehoben wird.	– Rollen und Verantwortlichkeiten des Prozesses für rechtliche Sperrfristen werden klar definiert und bekannt gemacht. – Wenn die rechtliche oder behördliche Sperrfrist für einen geeigneten Archivbestand aufgehoben wurde, beginnt der normale Vernichtungsprozess.	1. Es gibt keinen Prozess für rechtliche Sperrfristen. 2. Der Prozess für rechtliche Sperrfristen wird nicht befolgt. 3. Protokolle für rechtliche Sperrfristen werden befolgt, aber die normale Vernichtung beginnt nicht rechtzeitig nach Aufhebung der Sperrfrist. 4. Protokolle für rechtliche Sperrfristen werden befolgt, und der Vernichtungsprozess beginnt mit der Aufhebung der Sperrfrist.
Vernichtung von veralteten, ungültigen und temporären oder unbedeutenden Informationen	Veraltete, ungültige oder unbedeutende Informationen setzen Ihr Unternehmen einem unnötigen Sicherheitsrisiko und Rechtsstreitigkeiten aus. Zudem führen Archivbestände, die länger als notwendig aufbewahrt werden, zu Kosten in Form von Verwaltungs- oder IT-Belastungen. Fristgerechte Vernichtung (Entsorgung von veralteten, ungültigen und temporären oder unbedeutenden Informationen) hat positive Auswirkungen auf den Gewinn.	– Mit der Alterung der meisten Archivbestände nimmt deren Wert ab und ihr Risiko zu. Die meisten Unternehmen erfüllen die Anforderungen für die Aufbewahrung von Archivbeständen, zögern aber, veraltete, ungültige und temporäre oder unbedeutende Informationen zu entsorgen. – Die Unfähigkeit, eine Entscheidung zu treffen, ob Inhalte erhalten werden sollen oder nicht, und eine Unschlüssigkeit hinsichtlich der Entsorgung von geeigneten Archivbeständen bedeutet die Verwaltung von veralteten, ungültigen und temporären oder unbedeutenden Informationen und gefährdet sensible Informationen länger als dies von der Richtlinie vorgeschrieben ist. – Die Einführung von Datenanalytik ist jetzt ein wichtiger Faktor in einem effizient geführten und wettbewerbsorientierten Unternehmen, zusätzlich zur Vermeidung unnötiger Rechtsstreitigkeiten.	1. Es existiert kein Prozess zur Entsorgung von veralteten, ungültigen und temporären oder unbedeutenden Informationen. 2. Geschäftsbereiche definieren Archivbestände von Wert isoliert voneinander – Archivbestände werden länger als von der Richtlinie vorgesehen aufbewahrt. 3. Wertvolle Archivbestände werden identifiziert, und die Vernichtung von veralteten, ungültigen und temporären oder unbedeutenden Informationen findet umfassend statt, aber die Einhaltung wird nicht immer dokumentiert oder ist im gesamten Unternehmen nicht immer einheitlich. 4. Ein Information-Governance-Gremium (mit Mitgliedern aus verschiedenen Unternehmensabteilungen) kommt zu einem Einvernehmen zur Durchführung einer rechtlich durchsetzbaren Vernichtung im gesamten Unternehmen, und veraltete, ungültige und temporäre oder unbedeutende Informationen werden routinemäßig auf konforme Weise entsorgt.

RECHTLICHE SPERRFRISTEN

Rechtliche Sperrfristen werden verwendet, um die Aufbewahrungsfristen auszusetzen und die Vernichtung bestimmter Gruppen von Archivbeständen einzustellen, selbst wenn diese zur deren Aufbewahrungsfrist abgelaufen ist.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Richtlinie und Prozess für rechtliche Sperrfristen	Die Rechtsabteilung in Zusammenarbeit mit Compliance, IT und Archiv- und Informationsmanagement erstellt und implementiert einen lückenlosen Prozess für rechtliche Sperrfristen, der Richtlinien und Verfahren zur Durchsetzung von Aufbewahrungspflichten für Papierakten und elektronische Archivbestände umfasst. Leistungsmaßstäbe, Rollen und Verantwortlichkeiten werden klar dokumentiert, einschließlich der Angaben des globalen Teams zur Verwaltung von Sperrfristen.	– Dokumentation des lückenlosen Prozesses für rechtliche Sperrfristen entweder in einem Flussdiagramm oder einem sonstigen umfassenden Medium. – Der Prozess beinhaltet eine Methode zur Aussetzung der Vernichtung von Archivbeständen, die für Rechtsstreitigkeiten benötigt werden, und zur Aufhebung von Sperrfristen, wenn die Angelegenheit abgeschlossen ist. – Erstellung klar definierter Rollen und Verantwortlichkeiten für den Prozess für Sperrfristen: Festlegung eines globalen Teams für Rechtsstreitigkeiten (nach Bedarf aus Rechtsabteilung, IT-Abteilung, Archiv- und Informationsmanagement, Geschäftsleitung sowie externe Anwälte/Rechtsberater) für jede Region. – Durchführung von Schulungen zum Prozess für Sperrfristen für Personen, die eine Rolle oder Verantwortlichkeiten innehaben.	1. Es existieren keine formellen Prozesse, Richtlinien oder Verfahren für rechtliche Sperrfristen. 2. Ein Prozess für rechtliche Sperrfristen existiert, aber es gibt keine Richtlinie, die formelle Rollen und Verantwortlichkeiten definiert. 3. Ein Prozess für rechtliche Sperrfristen und eine Richtlinie existieren, aber es gibt keine formell definierten Rollen und Verantwortlichkeiten. 4. Ein lückenloser Prozess für rechtliche Sperrfristen mit entsprechenden Richtlinien und Verfahren einschließlich Rollen und Verantwortlichkeiten existiert und wird regelmäßig nach Bedarf aktualisiert. Teilnehmer erhalten Schulungen.
Verwaltung von Sperrfristen	Die Rechtsabteilung, Archiv- und Informationsmanagement, Compliance-Abteilung und IT-Abteilung müssen gemeinsam eine zentrale Stelle für die Verwaltung von rechtlichen oder sonstigen Sperrfristen gemäß der Richtlinie und dem Prozess für rechtliche Sperrfristen bilden oder auswählen und überwachen.	– Ein zentrales System enthält Informationen zu Sperrfristen, wie z. B.: Identifikationscode der Sperrfrist, Verwalter, Anwendungseigentümer, Anwendungen, Inhalt des Archivbestands und Funktionen der Systeme/Prozesse, die Identifikation und/oder Zurückhaltung von potenziell auffindbaren Informationen verhindern könnten. – Archiv- und Informationsmanagement hilft bei der Auswahl und Unterhaltung einer Anwendung zur Verwaltung von Sperrfristen.	1. Es gibt keine aktive Verwaltung von Sperrfristen. 2. Sperrfristen werden manuell durch mehrere Bereiche oder Geschäftseinheiten verwaltet. 3. Der Prozess für Sperrfristen wird manuell durch eine zentrale Stelle verwaltet. 4. Es existiert ein zentrales System oder eine zentrale Anwendung zur Verwaltung von Sperrfristen.
Umsetzung der Sperrfristen	Archiv- und Informationsmanagement muss mit den Teams für Rechtsstreitigkeiten eng zusammen arbeiten, um Einheitlichkeit, Vollständigkeit und Einhaltung des Prozesses für rechtliche Sperrfristen zu gewährleisten.	– Archiv- und Informationsmanagement unterstützt die Aufbewahrung und das Auffinden der Archivbestände, Entfernung von nicht mehr nötigen Sperrfristen sowie die Rückführung von Archivbeständen zu ihrer normalen, gewöhnlichen Aufbewahrungsfrist gemäß dem Aufbewahrungsplan des Unternehmens basierend auf Anweisungen des Koordinators für rechtliche Sperrfristen. – Archiv- und Informationsmanagement arbeitet eng mit Geschäftsbereichen und der IT-Abteilung zusammen, um sicherzustellen, dass entsprechende Maßnahmen sowohl bei der Verhängung als auch der Aufhebung von Sperrfristen ergriffen werden.	1. Es gibt keine rechtlichen Sperrfristen. 2. Rechtliche Sperrfristen werden ohne Einbeziehung des Archiv- und Informationsmanagements verhängt und aufgehoben. 3. Es gibt keinen Koordinator für rechtliche Sperrfristen. Das Team für Rechtsstreitigkeiten arbeitet in Bezug auf Sperrfristen unmittelbar mit dem Archiv- und Informationsmanagement zusammen. 4. Der Prozess für rechtliche Sperrfristen wird von allen notwendigen Parteien vollumfänglich befolgt. Archiv- und Informationsmanagement ist aktiv an der Verhängung und Aufhebung von Sperrfristen beteiligt und arbeitet unter der Leitung des Koordinators für rechtliche Sperrfristen.
Umfang der Sperrfristen	Das Archiv- und Informationsmanagementprogramm hilft sicherzustellen, dass Sperrfristen so eng wie möglich bemessen werden. Von weitgreifenden pauschalen Sperrfristen wird abgeraten, außer wenn absolut notwendig.	– Die Stelle, die die Sperrfrist verhängt, sollte möglichst strukturierte Gespräche und Befragungen einsetzen, um im Laufe einer Angelegenheit den Umfang der relevanten Dokumente/Daten feststellen zu können. – Erfassung der Ergebnisse in zentraler Datenbank. – Sicherstellen, dass Mitteilungen zu rechtlichen Sperrfristen von Anwälten schriftlich und in folgender Form verfasst werden: • Mitteilung unterstützt Personen beim Ergreifen von Maßnahmen und liefert zusätzliche Anleitung (z. B. Sperrfrist mit Archivbestandskategorien des Aufbewahrungsplans für Archivbestände abgleichen). • Mitteilung basiert auf Vorlagen für eine klare Kommunikation von Anweisungen sowohl am Anfang als auch wenn der Umfang zu- oder abnimmt.	1. Es gibt keinen Prozess für rechtliche Sperrfristen. 2. Pauschale Sperrfristen sind die Norm. 3. Es werden Anstrengungen unternommen, pauschale Sperrfristen zu verhindern und/oder aktuelle pauschale Sperrfristen von unwichtigen Archivbeständen zu entfernen. 4. Sperrfristen beziehen sich nur auf Archivbestände, die als relevant für die Angelegenheit angesehen werden.

DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Kontrollen für Datenschutz und Informationssicherheit beziehen sich auf die Maßnahmen, die notwendig sind, um Information in Übereinstimmung mit Gesetzen, Vorschriften und betrieblichen Anforderungen während ihres gesamten Lebenszyklus zu schützen.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Datenklassifizierung	Informationen werden nach Sensibilität und Wert für das Unternehmen klassifiziert. Kontrollen für die Informationssicherheit müssen entsprechend der Klassifikation der Daten aufgestellt werden.	– Beispiele für Datenklassifizierung: • „Streng vertraulich", was personenbezogene Informationen beinhaltet • „Vertraulich", „Eingeschränkt zugänglich" oder „Nur zum internen Gebrauch" • „Nicht eingeschränkt" oder „Öffentlich"	1. Es existiert keine Datenklassifizierung und keine Datenschutzrichtlinie oder ein Datenschutzprozess. 2. Es gibt keine formellen Protokolle zur Informationsklassifizierung, aber sensible Daten werden auf irgendeine Weise geschützt. 3. Es gibt keine formellen Protokolle zur Informationsklassifizierung, aber sensible Daten werden auf irgendeine Weise geschützt. Unternehmensdaten werden nur teilweise klassifiziert und geschützt. Der Schutz konzentriert sich auf personenbezogene Daten und sonstige streng vertrauliche Informationen. 4. Alle Informationen im Unternehmen werden klassifiziert, und Datenschutzkontrollen entsprechend der Sensibilität und des Werts der Informationen sind vorhanden.
Sicherer Zugriff	Um Informationen sicher aufzubewahren, müssen Maßnahmen zum Schutz von Informationen in allen Formaten getroffen werden. Die Archiv- und Informationsmanagementrichtlinie kann diese Maßnahmen beinhalten oder sie können in einer separaten Richtlinie zum Informationsschutz enthalten sein.	– Systeme müssen mit Zugriffskontrollen geschützt werden, die den Schutz durch Passwörter beinhalten. – Passwörter müssen ein Format haben, das schwierig zu erraten ist, um zusätzlichen Schutz zu bieten. Beispiel für ein akzeptables Format: Passwort muss einzigartig sein, mindestens 8 Zeichen beinhalten, mindestens einen Buchstaben und eine Zahl oder ein Sonderzeichen (!,@,#,£,%,^,&,*,[,]) aufweisen. – Passwörter sollten regelmäßig geändert werden. – Nach einer bestimmten Zeit der Inaktivität, werden automatische Bildschirmschoner aktiviert. – Physische Archivbestände werden in einer geschützten und sicheren Umgebung aufbewahrt, was verschließbare Lagersysteme und Schlüsselkartenzutritt für Lagerbereiche einschließt.	1. Der Zugriff auf Systeme ist passwortgeschützt. Es gibt keine Kontrollen zum Schutz von Archivbeständen in Papierform. 2. Der Zugriff auf Systeme ist passwortgeschützt. Archivbestände in Papierform werden an verschiedenen Orten aufbewahrt, könnten aber nicht immer angemessen gesichert sein. 3. Der Zugriff auf Systeme ist passwortgeschützt, Benutzer werden gebeten, ihren Computer mit der Funktion Strg/Alt/Entf zu sperren, wenn er nicht in Verwendung ist. Archivbestände in Papierform werden in abschließbaren Schränken/Räumen/Standorten aufbewahrt. 4. Der Zugriff auf Systeme ist durch schwierig zu erratende Passwörter geschützt, automatische Bildschirmschoner werden nach 10-15 Minuten Inaktivität aktiviert, Archivbestände in Papierform werden in abschließbaren Schränken/Räumen/Standorten mit Schlüsselkartenzutritt aufbewahrt.
Cybersicherheit	Um das Risiko eines Datenverlusts zu minimieren, müssen ausreichende und angemessene Präventionsmaßnahmen umgesetzt werden. Die Archiv- und Informationsmanagementrichtlinie kann diese Datenschutzprotokolle beinhalten oder sie können in einer separaten Richtlinie zur Informationssicherheit oder zum Datenschutz enthalten sein.	– Datenverschlüsselung für Daten bei der Übertragung und bei der Speicherung muss für sensible und private Informationen eingerichtet werden. – Verschlüsselung muss auf allen Mobilgeräten für den Fall eines Diebstahls aktiviert sein. – USB-Beschränkung auf Wechselmedien (Flash-Laufwerke, Laptops usw.) wird strengstens empfohlen.	1. Es gibt keine Richtlinien oder Tools für den Datenschutz. 2. Datenschutzrichtlinien existieren, aber Tools sind veraltet oder nicht vorhanden. 3. Tools für die Cybersicherheit sind vorhanden, sind aber nicht auf dem neusten Stand. Richtlinien existieren. 4. Die aktuellsten Tools und Prozesse für die Cybersicherheit sind vorhanden. Datenschutzrichtlinien existieren.
Sichere Vernichtung	Ein Zertifikat für die sichere Vernichtung wird eingeführt, um das Unternehmen vor einem Datenverlust aufgrund von Diebstahl oder unbeabsichtigter Veröffentlichung von vertraulichen Papierdokumenten zu schützen.	– Das Archiv- und Informationsmanagementprogramm entwickelt, veröffentlicht und implementiert eine Vernichtungsrichtlinie, die davon ausgeht, dass alle Papierakten vertraulich sind und aus diesem Grund vernichtet werden müssen.	1. Es gibt keine Vernichtungsrichtlinie. 2. Eine Vernichtungsrichtlinie ist nur für streng vertrauliche und vertrauliche Informationen vorhanden. 3. Es gibt eine Vernichtungsrichtlinie für Papierakten, die als „streng vertraulich", „vertraulich" oder „eingeschränkt zugänglich" markiert sind. 4. Es gibt eine Vernichtungsrichtlinie für alle Papierakten.
Entsorgung von Medien und elektronischen Abfällen (IT-Asset-Disposition)	Um den Schutz vor einem Datenverlust aufgrund von Diebstahl oder unbeabsichtigter Veröffentlichung von vertraulichen Informationen in verschiedenen Arten von Medien zu gewährleisten, enthält die Archiv- und Informationsmanagementrichtlinie oder eine separate Informationsschutzrichtlinie die Anforderungen für eine sichere Entsorgung von digitalen Medien.	– Aufstellung eines rechtlich durchsetzbaren, dokumentierten und wiederholbaren Prozesses zur Vorbereitung, zum Transport und zur Vernichtung von Festplatten, Backup-Medien und sonstigen elektronischen Abfällen entweder im Datenzentrum des Unternehmens oder in einer externen Vernichtungseinrichtung eines Drittanbieters. – Prüfung des Prozesses mit Zertifizierung der Nachweiskette und strenger Einhaltung der brancheninternen und lokalen Auflagen zur sicheren Entsorgung von IT-Geräten.	1. Es existiert kein formeller Prozess zur sicheren Vernichtung von Medien und elektronischen Abfällen. 2. Ein externer Drittanbieter wird beauftragt, der auf die sichere Entsorgung von Medien und elektronischen Abfällen spezialisiert ist. Es gibt keinen Prüfpfad. 3. Ein externer Drittanbieter wird beauftragt, der auf die sichere Entsorgung von Festplatten, Backup-Medien und sonstigen Hardware-Komponenten oder Geräten mit Informationen spezialisiert ist. Der Drittanbieterprozess ist lückenlos prüfbar mit Zertifizierung der Nachweiskette und endgültiger Entsorgung.
Berichterstattung zu Datenschutzverletzungen	Datenverletzungsereignisse werden aufgedeckt und dem zuständigen Notfallteam (Incident Response Team) zeitnah gemeldet. Ereignisse werden analysiert, um eine ordnungsgemäße Untersuchung, Eindämmung und Kontrolle zu gewährleisten. Gegebenenfalls werden Benachrichtigungen an Regulierungs- und Strafverfolgungsbehörden sowie betroffene Kunden versendet.	– Eine globale Datenschutzrichtlinie und eine Richtlinie zur Vorfallsmeldung existieren, die den Prozess der Verwaltung aller Schritte zur Meldung von Datenschutzverletzungen beschreiben.	1. Es existiert keine Richtlinie zur Datenschutzverletzung. 2. Richtlinien und Protokolle zur Datenschutzverletzung existieren, werden aber nicht konsequent eingehalten. Es gibt kein Notfallteam (Incident Response Team). 3. Richtlinien und Protokolle zur Datenschutzverletzung werden konsequent befolgt, aber es gibt kein koordinierendes Notfallteam (Incident Response Team). 4. Richtlinien und Protokolle zur Datenschutzverletzung werden konsequent befolgt. Es gibt ein Notfallteam (Incident Response Team).

LIEFERANTENMANAGEMENT

Die Auswahl und Verwaltung geeigneter Lieferanten ist zwingend notwendig, um sicherzustellen, dass Partner die Archiv- und Informationsmanagementrichtlinien und -standards des Unternehmens im Hinblick auf die Verwaltung von Archivbeständen und Informationen einhalten.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Due-Diligence-Überprüfung bei der Lieferantenauswahl	Das Archiv- und Informationsmanagementprogramm nimmt eine angemessene Due-Diligence-Überprüfung für jeden externen Partner vor, unter Einhaltung der Anforderungen der Archiv- und Informationsmanagementrichtlinie und des allgemeinen Beschaffungs-/Lieferantenauswahlprozesses des Unternehmens.	– Angemessene interne/externe Due-Diligence-Überprüfungen unter Einbeziehung aller notwendigen Bereiche (Risikomanagement, Rechtsabteilung, Archiv- und Informationsmanagement usw.) finden vor der Durchführung von Geschäften statt. – Es wird nachgewiesen, dass der Lieferanten die Anforderungen der Archiv- und Informationsmanagementrichtlinie im Hinblick auf die Lagerung, den Schutz, die sichere Vernichtung usw. erfüllt. Das schließt auch Standortbesuche, Referenzen usw. ein. – Ergebnisse der Due-Diligence-Überprüfungen werden dokumentiert.	1. Es gibt keinen formellen Due-Diligence-Prozess für die Sicherheitsüberprüfung von Lieferanten/Partnern des Archiv- und Informationsmanagements. 2. Eine Due-Diligence-Überprüfung findet statt, aber nicht alle Parteien werden einbezogen oder sie wird nicht vollständig dokumentiert. 3. Eine Due-Diligence-Überprüfung findet für alle relevanten Parteien statt, und sie wird vollständig dokumentiert. Es existiert kein Nachweis der Einhaltung. 4. Eine Due-Diligence-Überprüfung findet für alle relevanten Parteien statt, und sie wird vollständig dokumentiert. Nachweise werden erbracht, um zu beweisen, dass der Lieferant die Anforderungen des Archiv- und Informationsmanagements erfüllt.
Lieferantenbeurteilung	Das Archiv- und Informationsmanagementprogramm muss Dienstleistungsrisiken bemessen, Kontrollen beurteilen und die Leistung in Bezug auf Technologie, Betriebsabläufe, Partnerschaften und sonstige Lieferanten- und/oder Drittparteibeziehungen überwachen, wie externe Lagerung, die den Archiv- und Informationsmanagementprozess unterstützen. Ein unterzeichneter und gültiger Vertrag definiert den Umfang, die Verpflichtungen und Verantwortlichkeiten der Parteien. Die vom Lieferanten durchgeführten Dienstleistungen und deren Umfang werden planmäßig auf ihre Übereinstimmung mit den Vertragsbedingungen überprüft.	– Rollen und Verantwortlichkeiten werden zur Überwachung und Steuerung der Lieferanten definiert, was Entscheidungsfindung, Eskalation und Aufsicht beinhaltet. – Ein Dienstleistungsrisiko-Manager wird für die Verwaltung von täglichen Vertragsverpflichtungen bestimmt. – Nachweise existieren, einschließlich Standortbesuche zur Unterstützung der Überwachung der Lieferanten, die regelmäßige Sitzungsprotokolle umfassen, welche Dienstleistungsgespräche, Risiken, Probleme, Korrekturpläne, organisatorische Änderungen des Auftragnehmers und Finanzsituation dokumentieren. – Dienstleistungen werden in Übereinstimmung mit Outsourcing-, Audit- und aufsichtsrechtlichen Anforderungen verwaltet und überwacht.	1. Eine Risikobeurteilung von Archiv- und Informationsmanagementdienstleistern bzw. -lieferanten findet nicht statt. 2. Beurteilungen werden für einige Lieferanten durchgeführt, aber es gibt keine konsequente Verfolgung zur Korrektur. 3. Regelmäßige Beurteilungen aller Lieferanten werden durchgeführt, und Korrekturpläne werden dokumentiert und verfolgt. 4. Geplante und formelle Lieferantenbeurteilungen finden statt, und während dieser Zeit werden Dienstleistungen überprüft und Korrekturpläne dokumentiert und verfolgt.
Lieferantenkonsolidierung	Die Verwaltung mehrerer LieferantenPartner kann zu Schwierigkeiten bei der Durchsetzung einheitlicher Standards und best Practices führen. Sie kann wertvolle Zeit, Geld und Energie kosten, wenn es um Ressourcen und die Risiken geht, die das Unternehmen in Bezug auf Compliance und Rechtsstreitigkeiten eingeht. Ermittlung und Rechtsstreitigkeiten sind bedeutend schwieriger und zeitaufwendiger aufgrund mehrerer Formate und Aufbewahrungsorte der Archivbestände, was zu einer uneinheitlichen Vernichtung und verschiedenen Sperrfristen führen kann.	– Uneinheitliche Richtlinien und Aufbewahrungsverfahren setzen Ihr Unternehmen bedeutenden juristischen und finanziellen Risiken aus. Aufgrund der höheren System- und Personalanforderungen beim Einsatz mehrerer Lieferanten steigen Ermittlungs- und Verwaltungskosten. – Unternehmen mit einem einzigen Lieferanten haben Möglichkeiten, das organisatorische Risiko zu senken und zu beseitigen. – Best Practice: Reduzierung der Ermittlungszeit für Archivbestände und Verstärkung der Einhaltung und rechtlichen Durchsetzbarkeit durch Konsolidierung der Archivbestände in ein einziges System.	1. Es findet keine Konsolidierung der Lieferanten statt – es existiert keine Übersicht für Archivbestände/Partner. 2. Das Erstellen einer Übersicht zu Archivbeständen mehrerer Lieferanten ist vorgeschrieben, wird aber nicht immer dokumentiert. 3. Eine regelmäßige Bewertung aller Lieferanten wird durchgeführt, um die konsequente Anwendung der Richtlinie sicherzustellen. 4. Durch jeden Schritt der Konsolidierung wird ein Prozess aufgebaut. Konsequente Anwendung der Richtlinie und einheitliche Aufbewahrungsmethoden gewährleisten rechtzeitige Vernichtung.

PERSONAL

Personal bezieht sich auf die Mitarbeiter, die notwendig sind, um das Archiv- und Informationsmanagementprogramm an allen Standorten, zu verwalten und zu unterstützen, und zwar als unabhängige Funktion und innerhalb eines Geschäftsbereichs. Die Entwicklung, Bereitstellung und Überwachung von Schulungen für alle Mitarbeiter und andere (Auftragnehmer und Lieferanten), die Archivbestände und Informationen erstellen, empfangen und/oder verwalten, ist notwendig, um die Einhaltung der Archiv- und Informationsmanagementrichtlinie zu unterstützen.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Archiv- und Informationsmanagemen-tpersonal: Vollzeit	Das Archiv- und Informationsmanagementprogramm ist mit vollzeitbeschäftigten Personen besetzt, die nach Bedarf, weltweit tätig sind und von der Geschäftsleitung unterstützt und beaufsichtigt werden.	– Das Archiv- und Informationsmangement wird zentral gesteuert und ist mit der notwendigen Anzahl vollzeitbeschäftigter, geschulter/zertifizierter Personen besetzt, um die Umsetzung und Pflege des Programms sowie die Zusammenarbeit mit anderen Funktionen wie Rechts- und IT-Abteilung und den Geschäftsbereichen zu gewährleisten. – Wenn das Programm nicht zentralisiert ist, wird die Leitung bestimmten Personen übertragen, um das Programm und diesbezügliche Beziehungen zu entwickeln und zu verwalten.	1. Es wird kein Vollzeit-Personal für das Archiv- und Informationsmanagement beschäftigt. 2. Es existiert nur eine unzureichende Anzahl von vollzeitbeschäftigten, zentralisierten Mitarbeitern für das Archiv- und Informationsmanagement. Eine Unterstützung durch die Geschäftsleitung findet nicht statt. 3. Vollzeitbeschäftigtes zentralisiertes Personal für das Archiv- und Informationsmanagement existiert, aber nur in einer unzureichenden Anzahl, um effektiv zu sein. Es findet eine minimale Unterstützung durch die Geschäftsleitung statt. 4. Vollzeitbeschäftigtes, zentralisiertes, geschultes und zertifiziertes Personal für das Archiv- und Informationsmanagement existiert in ausreichender Anzahl, um das Programm durchzuführen, und es wird von der Geschäftsleitung unterstützt.
Archiv- und Informationsmanagemen-tpersonal: Netzwerk (Teilzeit)	Das Personal in den Geschäftsbereichen wird vor Ort zur Unterstützung des zentralen Archiv- und Informationsmanagementprogramms zusätzlich zu deren Vollzeitbeschäftigung eingeteilt. Diese Rolle als Archivkoordinator oder Archivkontakt des Geschäftsbereichs wird in der Archiv- und Informationsmanagementrichtlinie als eine Voraussetzung vorgeschrieben, die Geschäftsbereiche erfüllen müssen, um Compliance zu gewährleisten.	– Die Rolle eines dezentralisierten Geschäftsbereich-Koordinators wird geschaffen und erhalten. – Personal wird eingeteilt, um das zentrale Programm zu unterstützen. – Änderungen des Geschäftsbereich-Koordinators werden dem zentralen Personal für das Archiv- und Informationsmanagement gemeldet. – Die Verantwortlichkeiten des Archiv- und Informationsmanagements werden in den jährlichen Zielsetzungen des Koordinators berücksichtigt.	1. Es existiert kein Personal für das Archiv- und Informationsmanagement in den Abteilungen. 2. Es gibt Unterstützungspersonal in den Abteilungen ohne Verbindung zum zentralen Programm. 3. Einige aber nicht alle Abteilungen haben unterstützendes Personal. Offene Kommunikationswege mit dem zentralen Programm existieren. 4. Dezentralisiertes Personal der Abteilungen wird in unterstützender Funktion eingesetzt. Offene Kommunikationswege mit dem zentralen Programm existieren.

SCHULUNG

Die Entwicklung, Bereitstellung und Überwachung von Schulungen für alle Mitarbeiter und andere (Auftragnehmer und Lieferanten), die Archivbestände und Informationen erstellen, empfangen und/oder verwalten, ist notwendig, um die Einhaltung der Archiv- und Informationsmanagementrichtlinie zu unterstützen.

KONTROLLE	BESCHREIBUNG	UNTERSTÜTZENDE INFORMATIONEN	BEWERTUNG
Entwicklung von Schulungs- und Kommunikationsplänen und -materialien	Angemessene Schulungspläne und -materialien werden entwickelt, gepflegt und von einer zuständigen Person oder Funktion genehmigt. Ständige Kommunikation findet statt, um Schulungen zu untermauern und über Konformitätsanforderungen, Richtlinienänderungen usw. zu informieren. Das Archiv- und Informationsmanagementprogramm sollte als Grundlage für jede Archiv- und Informationsmanagementschulung dienen.	– Schulungsmaterialien müssen regelmäßig auf Richtigkeit überprüft werden, und Anträge auf Änderungen sind bei der zuständigen Person oder Funktion einzureichen. – Zusammenarbeit mit dem Kommunikationsteam, um zu gewährleisten, dass Mitarbeiter zu Richtlinienänderungen auf dem neuesten Stand gehalten werden. – Wenn kein Kommunikationsteam existiert, muss ein Plan zur Schaffung von Bewusstsein entwickelt und eingeführt werden.	1. Es existieren keine Pläne und Materialien für eine Archiv- und Informationsmanagementschulung. 2. Pläne und Materialien sind veraltet und werden ad hoc eingesetzt. 3. Pläne und Materialien sind aktuell und genehmigt. Kommunikation ist sporadisch oder findet nicht statt. 4. Pläne und Materialien sind aktuell und werden regelmäßig überprüft. Vollzeitbeschäftigtes Personal stellt sicher, dass die Kommunikation mit allen Mitarbeitern kontinuierlich stattfindet.
Schulung und Überwachung	Es existieren Nachweise zu Benachrichtigungen hinsichtlich der Teilnahme an Schulungskursen und des erfolgreichen Abschlusses von Kursen. Die Einhaltung der geforderten Schulungspläne wird überwacht, und die Teilnahme wird durch Schulungssponsoren durchgesetzt.	– Bestätigung der Richtigkeit der Liste von Schulungsteilnehmern. – Erbringung von Nachweisen, einschließlich Originalliste der Schulungskandidaten mit Angabe, ob Kurs abgeschlossen wurde oder nicht, zusammen mit Kommunikation und Weiterverfolgung an zentralem Ablageort.	1. Es finden keine Schulungen statt. 2. Sporadische Schulungen und keine einheitliche Durchsetzung des erfolgreichen Schulungsabschlusses. 3. Ausgewählte zu schulende Mitarbeiter haben Kurse erfolgreich mit Nachweisen abgeschlossen. 4. Alle Mitarbeiter haben Kurse erfolgreich mit Nachweisen abgeschlossen.

Es ist wichtig, anzumerken, dass die meisten regulierten Unternehmen von jedem Geschäftsbereich verlangen, ein Risk Control Self-Assessment (RCSA, Selbstbeurteilung von Risiken und internen Kontrollen) zu entwickeln, mit dem alle Risiken dokumentiert, bewertet und quantifiziert werden, denen das Unternehmen ausgesetzt ist.

INSTITUTIONALISIERUNG

Das Risikomanagementsystem für das Archiv- und Informationsmanagement soll Unternehmen dabei helfen, die Einhaltung von Gesetzen und Vorschriften bezüglich Archivbeständen in allen ihren Geschäftsbereichen und Standorten zu verwalten. Das geschieht durch die Aufstellung und Einführung einer Reihe von Kontrollen, die zur Minderung einer Vielzahl von Risiken für Archivbestände und Informationen dienen.

Das Archiv- und Informationsmanagement-Team Ihres Unternehmens muss die vorgeschlagenen Kontrollen überprüfen, um festzustellen, welche für Ihre spezifische Geschäftstätigkeit angemessen sind. Es wird strengstens empfohlen, dass die ausgewählten Kontrollen mit anderen Teams innerhalb Ihres Unternehmens besprochen werden, wie z. B. die Compliance- und die Rechtsabteilung, Informationssicherheit und Risikomanagement, um eine einheitliche Vorgehensweise, das Einholen ihrer Zustimmung und eine Vermeidung potenzieller Überflüssigkeit ihrer Initiativen zu gewährleisten.

Sobald eine Vereinbarung zu den Kontrollen getroffen wurde, muss das Archiv- und Informationsmanagement-Team die Geschäftsbereiche über den Zweck dieser Kontrollen, den Prozess zur Durchführung dieser Kontrollen, die Anweisungen zur einheitlichen Bewertung des Archiv- und Informationsmanagementrisikos und sonstige sachdienliche Einzelheiten informieren. Online-Zugriff auf diese wertvollen Informationen ermöglicht deren Verteilung zu Beginn der Selbstbeurteilungen und zur ständigen Referenz. Sie können die Durchführung eines „Testdurchlaufs“ mit einem oder zwei Geschäftsbereichen in Betracht ziehen, bevor Sie die Selbstbeurteilung im gesamten Unternehmen einführen.

Es ist wichtig, anzumerken, dass die meisten Unternehmen von jedem Geschäftsbereich verlangen, ein Risk Control Self-Assessment (RCSA, Selbstbeurteilung von Risiken und internen Kontrollen) zu entwickeln, mit dem alle Risiken dokumentiert, bewertet und quantifiziert werden, denen das Unternehmen ausgesetzt ist. Die im vorhergehenden Abschnitt beschriebenen Archiv- und Informationsmanagementkontrollen sind ein sehr wichtiger Teil dieses RCSA-Dokuments.

RAHMENPLAN-ÜBERSICHT

Die Selbstbeurteilungen des Archiv- und Informationsmanagementrisikos durch die Geschäftsbereiche müssen jährlich (oder wie anderweitig bestimmt) durchgeführt werden. Um zu gewährleisten, dass diese mit den Compliance-Anforderungen übereinstimmen und wichtige geschäftliche Änderungen widerspiegeln, ist es unerlässlich, einen formellen Prozess zur Überprüfung und Verwaltung aufzustellen.

Nachfolgend finden Sie eine Beschreibung einer mehrstufigen Methode zur Aktualisierung und Einholung von Genehmigungen durch relevante und befugte Parteien, z. B. Archiv- und Informationsmanagement, Compliance und globale Geschäftsbereiche, um zu bestätigen, dass die Risikobewertungen sowie deren Systeme zur Umsetzung angemessen bleiben.

Jährlich:

- Neue Risiken identifizieren, Kontrollen hinzufügen oder modifizieren
- Anwendbarkeit der derzeitigen Kontrollen bestätigen und nach Bedarf bearbeiten
- Beiträge der Geschäftsbereiche hinsichtlich der Benutzerfreundlichkeit des Erfassungstools, der Relevanz der Kontrollen und des Bewertungssystems überprüfen
- Angemessene Änderungen des Prozesses zur Beurteilung des Archiv- und Informationsmanagementrisikos vornehmen
- Methodik überwachen

Quartalsweise:

- Funktionsweise der Kontrollen beurteilen
- Nach Bedarf Änderungen empfehlen

Fortlaufend:

- Lücken im Aufbau und der Durchführung der Beurteilungen des Risiko- und Kontrollrahmens für das Archiv- und Informationsmanagement identifizieren
- Input der Geschäftsbereiche einholen
- Nach Bedarf Änderungen empfehlen

Es ist wichtig, die getroffenen Entscheidungen zur Bearbeitung oder Änderung der Risikokontrollen für das Archiv- und Informationsmanagement und deren Verteilung an die Geschäftsbereiche zu dokumentieren. Es muss auf die Einhaltung der Häufigkeit der Überprüfungen, die Erstellung eines Aktionsplans für den Fall, dass geplante Zeiten verpasst wurden, und die zeitnahe Erfassung neuer oder sich entwickelnder Risikoereignisse geachtet werden. Je nach den Bedürfnissen eines Unternehmens kann ein weniger strenger Plan zur Überprüfung der Risikokontrollen für das Archiv- und Informationsmanagement ausreichend sein.

UMSETZUNGSMETHODE

Die Datenerfassung im Rahmen der Selbstbeurteilung des Archiv- und Informationsmanagementrisikos sollte einen Nachweis über die Einhaltung durch die Geschäftsbereiche beinhalten.

Die Selbstbeurteilungen des Archiv- und Informationsmanagementrisikos sollten an zuständige Geschäftsbereiche elektronisch übermittelt werden. Dies kann beispielsweise in Form des Online-Fragebogentools SurveyMonkey® oder einer ähnlichen Anwendung stattfinden, die eine interaktive Benutzererfahrung mit einer Anleitung zur Teilnahme innerhalb eines vorgeschriebenen Zeitrahmens ermöglicht. Es muss auch einen Bericht über die Ergebnisse beinhalten, damit diese ausgewertet und beurteilt werden können. Alternativ können Excel®-Tabellen, Word-Dokumente, E-Mails und/oder persönliche Gespräche andere Optionen für die Verteilung, Verfolgung von Teilnahmezeiten und Erfassung der Bewertungen sein. Um die notwendigen Ressourcen für die Auswertung der Antworten der Geschäftsbereiche zu steuern, wird empfohlen, die Selbstbeurteilungen des Archiv- und Informationsmanagementrisikos auf das ganze Jahr gestaffelt zu verteilen. Das ermöglicht eine Einplanung von Spitzenlastzeiten in einem Kalenderjahr für bestimmte Geschäftsbereiche.

> **Ein spezieller „Sponsor der Geschäftsleitung“ muss ausgewählt werden, um die Programmaufsicht und -leitung zu übernehmen, und Ihnen eine Stimme bei Besprechungen mit der Geschäftsleitung zu verleihen. Logische Sponsoren sind zum Beispiel Chief Compliance Officer, Chief Information Governance Officer oder Chief Information Officer.**

ROLLEN UND VERANTWORTLICHKEITEN

Es ist wichtig, die Kultur und Geschäftsstruktur Ihres Unternehmens zu bedenken, um zu verstehen, mit wem Sie als Archiv- und Informationsmanagement-Spezialist zusammenarbeiten müssen, um den Erfolg der Umsetzung Ihres Risikomanagementsystems für das Archiv- und Informationsmanagement zu garantieren.

Die Unterstützung der meisten Führungskräfte Ihres Unternehmens ist notwendig, um die Wichtigkeit und die erwartete Einhaltung des Programms zu unterstreichen. Dafür muss ein spezieller „Sponsor der Geschäftsleitung" ausgewählt werden, um die Programmaufsicht und -leitung zu übernehmen, und Ihnen eine Stimme bei Besprechungen mit der Geschäftsleitung zu verleihen. Logische Sponsoren sind zum Beispiel Chief Compliance Officer, Chief Information Governance Officer oder Chief Information Officer.

Im Folgenden finden Sie kurze Beschreibungen der typischen Haupt- und Nebenrollen für die Beurteilungen des Risikos und der Kontrollen des Archiv- und Informationsmanagement zusammen mit deren Verantwortlichkeiten. Diese Rollen können in Ihrem Unternehmen andere Bezeichnungen haben und/oder mit anderen Funktionen kombiniert sein, wie z. B. Rechts- und Compliance-Abteilung.

Sie können sich auch dazu entscheiden, die Verantwortlichkeiten der Haupt- und Nebenrollen zu verwenden, um die notwendigen Fähigkeiten für eine Stellenbeschreibung zu identifizieren, oder um ausgewählten Partnern dabei zu helfen, Sie bei Ihrem Archiv- und Informationsmanagementprogramm oder Ihrem allgemeinen Überprüfungsprogramm zu unterstützen.

HAUPTROLLEN:

Sponsor der Geschäftsleitung

- Trägt die allgemeine Verantwortung, um sicherzustellen, dass die Risikobeurteilungen des Archiv- und Informationsmanagements im gesamten Unternehmen durchgeführt werden
- Holt die Zustimmung der leitenden Führungskräfte aller Geschäftsbereiche und der Geschäftsführung ein
- Unterstützt den Leiter des Archiv- und Informationsmanagements, wenn die Geschäftsbereiche nicht die Maßnahmenpläne befolgen, um die Einhaltung zu gewährleisten

Leiter des Archiv- und Informationsmanagements

- Beaufsichtigt das Risikobeurteilungsprogramm des Archiv- und Informationsmanagements
- Arbeitet mit den Geschäftsbereichen zusammen, um die höchsten Risiken basierend auf Vorfällen und neu entstehende Risiken zu identifizieren
- Agiert als Fachexperte bei der Beurteilung der Effektivität der Risiken und Kontrollen
- Erstellt Maßnahmenpläne für Geschäftsbereiche, die die Vorgaben nicht eingehalten haben
- Setzt Korrekturmaßnahmen, -pläne und -lösungen zur Behebung von Problemen um
- Baut eine betriebliche Struktur, Prozesse, Kontrollen und notwendige Berichterstattung auf, um die Archiv- und Informationsmanagementrichtlinie zu befolgen
- Vertritt die Geschäftsbereiche in wichtigen unternehmensweiten Ausschüssen und Arbeitsgruppen zur Information Governance
- Stellt sicher, dass die Geschäftsbereiche Informationen und Schulungen zur Risikobeurteilung erhalten
- Unterstützt die Geschäftsbereiche bei der Einhaltung des Archiv- und Informationsmanagementprogramms
- Arbeitet mit Partnern zusammen: Risikomanagement, Compliance, Audit, IT usw., um den Erfolg des Programms zu gewährleisten

Geschäftsbereich-Manager / Abteilungsleiter

- Versteht gemeinsame Ziele und Verantwortlichkeiten zur Entwicklung und Durchführung der Archiv- und Informationsmanagementrichtlinien innerhalb des Unternehmens
- Baut Risikobewusstsein bezüglich der Archivbestände innerhalb des Unternehmens auf und dokumentiert mögliche Akten- oder Datenverluste
- Verteilt Kontrollvorgaben an zuständige Bereiche
- Führt die Risikobeurteilung des Archiv- und Informationsmanagements innerhalb des vorgegebenen Zeitrahmens durch
- Verwaltet Maßnahmenpläne, um die Schließung von Lücken im Kontroll- und Risikomanagement sicherzustellen
- Leitet das Archivprogramm des Geschäftsbereichs
- Befolgt das Risikobeurteilungsprogramm des Archiv- und Informationsmanagements
- Arbeitet mit dem zentralen Team und/oder den Geschäftsbereichsteams für das Archiv- und Informationsmanagement einschließlich der Archivkoordinatoren zusammen

NEBENROLLEN:

Diese Rollen können ausgewählt werden, um mit dem Programm zum Risikomanagementsystem des Archiv- und Informationsmanagements in den verschiedenen Phasen seiner Entwicklung, Einführung, Durchführung und Überwachung zusammenzuarbeiten. Sie können Änderungsempfehlungen dahingehend aussprechen, wie Kontrollen ausgewählt, beschrieben und/oder bewertet werden basierend auf ihrem speziellen fachlichen Verständnis Ihres Umfelds.

Rechtsabteilung

Die Aufgabe der Rechtsabteilung ist es, das Risikoprofil eines Unternehmens basierend auf der möglichen Gefährdung durch Rechtsstreitigkeiten, internationalen Datenschutzanforderungen, Schutz von geistigem Eigentum, Arbeitsumfeld usw. festzustellen. Sie sollte in die Auswahl und Formulierung der Kontrollen einbezogen werden, die für Ihr Unternehmen als geeignet angesehen werden.

Ermittlungsteam

Das Ermittlungsteam ist für die Kommunikation, Anweisung und Koordinierung mit Geschäftseinheiten und/oder Einzelpersonen bezüglich der Informationen verantwortlich, die aufgefunden und vorgelegt werden müssen, um Anforderungen von Rechtsstreitigkeiten nachzukommen. Diese Funktion führt einen wiederholbaren Prozess mit entsprechenden Vorgaben ein, um das gesamte Spektrum aller Rechtsstreitigkeiten von einfach bis schwierig zu verwalten, die sich auf rechtliche Sperrfristen innerhalb dieses Rahmenplans auswirken.

Risikomanagement

Das Risikomanagement ist für den Schutz der Marke, Finanzen und Betriebsabläufe des Unternehmens verantwortlich, indem es die Risikogefährdung verwaltet und mindert. Dieses Team bedarf eines vollständigen Verständnisses des Risikoprofils des Unternehmens (Rechtsstreitigkeiten, Ermittlungen, behördliche Auflagen, Schutz vertraulicher Informationen und geistigen Eigentums usw.) sowie der damit verbundenen Kontrollen. Es sollte eng in das Risikomanagementsystem für das Archiv- und Informationsmanagement eingebunden werden, um zu gewährleisten, dass die Kontrollen korrekt und aktuell sind.

Compliance

Die Compliance-Abteilung muss sicherstellen, dass dem Unternehmen die Anforderungen der von verschiedenen Behörden (Bundes-, Landes-/Kommunalbehörden, Regulierungsbehörden, Datenschutzbehörden, Branchengruppen usw.) auferlegten Regeln und Vorschriften bekannt sind und es diese befolgt. Sie sollte in die Festlegung interner Kennzahlen und Kontrollen involviert sein, am Aufbau eines unternehmensweiten Audit-Programms mitarbeiten und auf Anfragen von Regulierungsbehörden, Auditoren, Ermittlern, Kunden und anderen Drittparteien antworten und diese verwalten. Damit leistet die Compliance-Abteilung einen wichtigen Beitrag zu effektiven Risikokontrollen für das Archiv- und Informationsmanagement in Ihrem Unternehmen.

Informationstechnologie

Das IT-Team richtet sich immer mehr an den Geschäftsbereichen und deren Zielen aus. Es kann Beiträge zu den Kontrollen für das Archiv- und Informationsmanagement liefern, die sich mit dem ordnungsgemäßen Schutz und der Authentifizierung von Daten beschäftigen sowie deren Verfügbarkeit zur Nutzung, Erhaltung und Disposition.

Datenschutz

Die Datenschutz-Abteilung ist für die Verwaltung der Risiken und betrieblichen Auswirkungen von Datenschutzgesetzen und -vorschriften verantwortlich, sowie das Reagieren auf Bedenken von Regulierungsbehörden und Kunden hinsichtlich der Verwendung personenbezogener Daten einschließlich medizinischer Daten und finanzieller Informationen, sowie Gesetzen und Vorschriften für die Verwendung und den Schutz von Finanz- und Banktransaktionen mit Kunden. Mit dieser Abteilung kann Rücksprache gehalten werden hinsichtlich der ordnungsgemäßen Sicherung spezieller „risikoreicher" Informationen und deren Auswirkungen auf die Kontrollen für das Archiv- und Informationsmanagement.

Informationssicherheit

Das Informationssicherheits-Team ist für die Entwicklung, Umsetzung und Verwaltung der Sicherheitsvision, -strategie, -richtlinie und -programme des Unternehmens verantwortlich. Diese Abteilung ist verantwortlich für die Erstellung von Richtlinien, Auswahl und Einführung von Technologie, Überwachung und Information von Parteien über Malware, Datensicherheitsverletzungen, Hacking usw. sowie für die Erteilung von Codes zur Datenklassifizierung (zusammen mit der Rechtsabteilung). Sie sollte die sicherheitsbezogenen Kontrollen für das Archiv- und Informationsmanagement auf Richtigkeit überprüfen.

Datenanalysten

Der Datenanalyst ist für die Auswahl, Erfassung, Analyse und Interpretation von Daten verantwortlich, um die Effektivität, Produktivität und den Gewinn eines Unternehmens zu erhöhen. Für diese Aufgabe sind betriebswirtschaftliche Kenntnisse, ein technisches Verständnis von Computern und Datensystemen sowie die Fähigkeit zur Interpretation großer Datenmengen mittels Datenanalytik- und Visualisierungstools notwendig. Der Datenbeauftragte muss eng mit anderen zusammenarbeiten, um die Einhaltung der Datenschutzanforderungen bei der Verwendung von Daten über ihren ursprünglichen Zweck hinaus zu gewährleisten.

Internationale Vertretung

Da sich die Risiken für das Archiv- und Informationsmanagement über das gesamte Unternehmen erstrecken, muss es eine ordnungsgemäße Vertretung der globalen Funktionen bei der Erstellung, Umsetzung und fortwährenden Durchführung des Risikomanagementsystems für das Archiv- und Informationsmanagement geben. Diese internationale Vertretung kann die Form einer Delegation aus einer Region annehmen (z. B. aus dem Asien-Pazifik-Raum, EMEA und Nordamerika), die sich zu den Bedenken der unterschiedlichen Gerichtsbarkeiten innerhalb der Region äußern kann.

Personalabteilung/Mitarbeiterkommunikation

Je nach Struktur Ihres Unternehmens kann die Personalabteilung und/oder die Abteilung für Mitarbeiterkommunikation bei der ordnungsgemäßen Einführung des Risikoprogramms für das Archiv- und Informationsmanagement im gesamten Unternehmen helfen, indem sie Schulungsmaterialien entwirft, Rat zu Umsetzungsmechanismen und Übersetzungsanforderungen bietet und eine fortwährende Kommunikation über das Programm gewährleistet.

Metriken für die Risikokontrollen für das Archiv- und Informationsmanagement sollten regelmäßig identifiziert, erfasst und überprüft werden. Diese konsequente Datenerfassungsmethode ermöglicht Richtwerte und Präzisierung für Ihr Archiv- und Informationsmanagementprogramm, was fortwährende Investitionen und Ressourcenbeschaffung ermöglicht und das Bewusstsein der Geschäftsleitung, sowie die Übernahme des Archiv- und Informationsmanagements und der Information Governance fördert.

ERFOLGSMESSUNG

Die Einhaltung der Richtlinien und Verfahren des Archiv- und Informationsmanagements durch die Geschäftsbereiche muss überwacht, der Geschäftsleitung gemeldet und in geeigneten Risiko- und Governance-Foren besprochen werden.

Nachfolgend finden Sie einige Beispiele für Maßnahmen, die auf ein erfolgreiches Risikomanagementsystem für das Archiv- und Informationsmanagement hinweisen:

- Verbesserte Bewertungen der Geschäftsbereiche Jahr für Jahr
- Verbesserte unternehmensweite Leistungs- und Risikokennzahlen infolge einer umfassenderen Einhaltung der Richtlinie
- Erhöhtes Mitarbeiterbewusstsein zur Archiv- und Informationsmanagementrichtlinie und deren Anforderungen
- Keine behördliche Kritik
- Vermeidung der Schädigung Ihrer Marke

Metriken für die Risikokontrollen für das Archiv- und Informationsmanagement sollten regelmäßig identifiziert, erfasst und überprüft werden. Diese konsequente Datenerfassungsmethode ermöglicht Richtwerte und Präzisierung für Ihr Archiv- und Informationsmanagementprogramm, was fortwährende Investitionen und Ressourcenbeschaffung ermöglicht und das Bewusstsein der Geschäftsleitung, sowie die Übernahme des Archiv- und Informationsmanagements und der Information Governance fördert.

Wir empfehlen Ihnen, die oben genannte Liste angesichts der spezifischen Fähigkeiten und Methoden Ihres Unternehmens zur Datenerfassung und -analyse zu ändern und zu erweitern.

AKTIONSPLAN ZUR VERBESSERUNG

Der erste Schritt zur Verbesserung Ihres Risikoprofils für das Archiv- und Informationsmanagement ist es, die Bewertung auszuwerten um beurteilen zu können, wo Ihr Unternehmen steht. Wenn Sie Ihr Selbstbeurteilungsergebnis bestimmt haben, kann es notwendig sein, einen Aktionsplan zu erstellen, um das gesamte Ergebnis für das Archiv- und Informationsmanagementrisiko oder das Ergebnis einer bestimmten Kontrolle zu verbessern.

FRAGEN SIE SICH SELBST:

Welche der Risiken stellen die größte Bedrohung für Ihr Unternehmen dar, und welche der Kontrollen müssen sofort verbessert werden, um offensichtliche Lücken in Bezug auf diese Risiken zu schließen?

Um einen Plan aufzustellen, der sich auf kritische Bereiche konzentriert, ist es hilfreich, die Reihenfolge der Korrekturschwerpunkte festzustellen. Eine Verbesserung der Bewertung von einer „Drei“ auf eine „Vier“ ist bei bestimmten Risiken vielleicht nicht so wichtig für Ihr Unternehmen wie eine Verbesserung von einer „Zwei“ auf eine „Drei“ in einem anderen Bereich.

Kann das Archiv- und Informationsmanagement-Team im Alleingang Änderungen einführen, um die Kontrollen zu verbessern, oder ist eine Partnerschaft mit einem anderen Funktionsbereich notwendig?

Das Archiv- und Informationsmanagement-Team kann beispielsweise das Verfolgungs- und Berichtsystem für Archivbestände allein verbessern, muss aber wahrscheinlich mit der Rechts- und Compliance-Abteilung zusammenarbeiten, um Verbesserungen an den Kontrollen für rechtliche Sperrfristen vorzunehmen. Denken Sie darüber nach, welche Partnerschaften notwendig sein könnten und wie Sie die Zustimmung dieser Partner einholen.

Welche Ressourcen sind notwendig, um die Kontrollen zu verbessern?

Sie müssen eventuell sicherstellen, dass das Budget für ein neues oder verbessertes Verfolgungssystem für Archivbestände vorhanden ist, wenn das aktuelle System nicht die ausreichende Kontrolle bietet, die für eine ordnungsgemäße Bestandsverfolgung notwendig ist. Oder Sie können sich dazu entschließen, einen externen Fachexperten zu beauftragen, der Ihnen dabei hilft, einen Plan zur Reduzierung des gesamten Risikos zu entwerfen.

Was ist das Kosten/Nutzen-Verhältnis für die Verbesserungen?

Entscheiden Sie, ob die Zeit, Anstrengungen und Kosten für die Verbesserung der Risikokontrolle es wert sind, um sicherzustellen, dass Sie sich nur auf erreichbare Ergebnisse konzentrieren. Ein gut durchdachter Aktionsplan enthält nicht nur die Korrekturschritte und die dafür notwendigen Ressourcen, sondern zieht auch die wichtigsten Vorteile für das Unternehmen in Betracht und zeigt klare Ergebnisse. Wenn Sie den Plan darauf beschränken, was in Anbetracht des Risiko- und Kontrollrahmens Ihres Unternehmens erreichbar und realistisch ist, dann können Sie im Laufe der Zeit messbare Erfolge vorweisen.

HOLEN SIE SICH HILFE

Wenn Sie mehr über Information Governance Datenanalyst erfahren möchten, können Ihnen die Fachexperten von Iron Mountain weiterhelfen. Einzelheiten finden Sie in den folgenden Leitfäden: **A Practical Guide to Information Governance (Ein praktischer Leitfaden zur Information Governance)** und **A Records and Information Managers' Guide to Assessing Performance Risk (Ein Leitfaden für den Archiv- und Informationsmanager zur Beurteilung von Leistungsrisiken)**.

Weitere Informationen erhalten Sie von Ihrem Iron Mountain Account Manager oder telefonisch unter: **0800 408 0000 (Deutschland)** **+43 (0) 2287 30 544 (Österreich)**.

IRON MOUNTAIN®

0800 408 0000 | IRONMOUNTAIN.DE
+43 (0) 2287 30 544 IRONMOUNTAIN.CO.AT

ÜBER IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) ist ein global führender Dienstleister für Lösungen im Bereich Archiv- und Informationsmanagement. Mehr als 220.000 Unternehmen weltweit vertrauen auf Iron Mountain und unsere Archivstruktur umfasst eine Grundfläche von mehr als 7,9 Millionen Quadratmetern in mehr als 1.400 Einrichtungen in 45 Ländern, die eigens für den Schutz und Erhalt dessen ausgelegt sind, was unseren Kunden am wichtigsten ist. Das Dienstleistungsportfolio von Iron Mountain umfasst Archivmanagement, Datenmanagement, Scanning und Digitalisierung sowie die sichere Aktenvernichtung, um Kunden bei der Verringerung ihrer Lagerkosten, der Compliance-gerechten Aufbewahrung und der effizienteren Nutzung ihrer Informationen zu unterstützen. 1951 gegründet, speichert und schützt Iron Mountain Milliarden von Informationen, darunter kritische Geschäftsdokumente, elektronische Informationen und medizinische Daten, sowie kulturelle und historische Artefakte. Weitere Informationen unter www.ironmountain.de www.ironmountain.co.at