Fachbeitrag

Wie sicher sind Ihre Projektinformationen?

Informationssicherheit im Projekt nach ISO 27001 mit PRINCE2©

Haben Sie, hat Ihre Organisation den Wert der im Unternehmen vorhandenen Informationen bereits für sich erkannt? Zu diesen Informationen gehören auch die in Projekten verwendeten, aber vor allem die neu entstehenden Informationen – unabhängig von Projektart oder Branche. Doch welche konkreten Maßnahmen haben Sie ergriffen, um diese Informationen zu schützen? Ist Informationssicherheit in Ihrer Organisation Chefsache oder nur Aufgabe der IT-Abteilung?

Informationssicherheit ist ein Managementthema und gewinnt sowohl aufgrund der wachsenden Bedrohung durch Internetkriminalität als auch durch die normativen und rechtlichen Entwicklungen zunehmend an Bedeutung. Die DIN ISO/IEC 27001:2017-06 "Informationstechnik - Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen" (DIN 2017) stellt Organisationen, die ihre Managementsysteme bereit für die Herausforderungen der Informationsgesellschaft machen wollen, einen Maßstab für Informationssicherheit zur Verfügung.

Die ISO 27001 fordert in Anhang A (A.6.1.5) (DIN 2015) explizit, dass die Informationssicherheit auch im Projektmanagement berücksichtigt werden muss. Die logische Konsequenz daraus ist, dass Unternehmen die Aspekte der Informationssicherheit in ihren Projektmanagementsystemen integrieren müssen – sowohl um zukunftsfähig zu sein, als auch um normative wie rechtliche Anforderungen erfüllen zu können, wie z.B. in Deutschland das IT-Sicherheitsgesetz (BSI2016) und das Energiewirtschaftsgesetz §11 Abs. 1a (BMJV 2017).

Autor

Stefanie Eilhardt

Dipl.-Informationswirtin, zertifizierte Projektmanagerin, Vorstandsmitglied des BPUG Deutschland e.V., Organisatorin diverser PRINCE2-Fachveranstaltungen und mehrfaches Mitglied in der Jury für die Vergabe des PRINCE2 Best Practice Awards

Kontakt: St.Eilhardt@im-ps.de

Mehr Informationen unter:
› projektmagazin.de/autoren

ähnliche Artikel

› Informationssicherheit – Wann ist die Projektleitung in der Pflicht?

sowie in der Rubrik:

› Mit Standards arbeiten
› PRINCE2
› Wissensmanagement
› Risikomanagement

Im Folgenden stelle ich Ihnen Ansätze vor, wie Sie die Anforderungen der ISO 27001 in Ihr Projektmanagementsystem (PMS) integrieren können. Als konkretes Beispiel verwende ich hierfür das international weit verbreitete PMS PRINCE2® (AXELOS 2017). Selbstverständlich können die hier beschriebenen Ansätze auch analog auf andere PMS übertragen werden.

Mangelnde Informationssicherheit gefährdet den Projekterfolg

Projektbeteiligte sind auf Informationen angewiesen, um Aufgaben ausführen, Produkte beschreiben und Entscheidungen treffen zu können. Entscheidend dafür ist, dass Informationen vollständig und korrekt verfügbar

sind. Zugleich dürfen diese Informationen nicht in die falschen Hände geraten. Ist dies nicht gewährleistet, kann das schwerwiegende Folgen für ein Projekt, das Unternehmen, die angeschlossenen Dienstleister und die Kunden haben. Die folgenden Beispiele illustrieren, wie wichtig in Projekten die Sicherheit von Informationen sowohl für den Projekt- als auch für den Unternehmenserfolg ist.

Fehlentscheidungen

Liegen unvollständige oder fehlerhafte Informationen vor, kann das zu Fehleinschätzungen (z.B. Dauer einer Aufgabe mit Auswirkung auf die geschätzte Projektdauer) und Fehlentscheidungen (z.B. durch unbekannte Risiken) führen, die sich langfristig auf Faktoren wie Kosten, Zeit und Qualität eines Projekts auswirken können.

Wiederbeschaffungsaufwände & Zusatzkosten

Kommen Informationen und ihre Datenträger abhanden und besteht keine entsprechende Sicherheitskopie, müssen Informationen neu generiert werden. Aufwände für die Neuanschaffung von Mobilgeräten wie Laptops und Handys belasten das Projektbudget.

Ineffizienter Ressourceneinsatz

Arbeiten Sie mit externen Mitarbeitern zusammen, kann die Nichtverfügbarkeit von Informationen zu Doppelarbeit und Aufwänden für die erneute Informationsbeschaffung führen, z.B. Erstellung einer Auswertung, die über das Projektbudget bezahlt werden müssen.

Terminverschiebungen & Planungsverzug

Stehen entscheidungsrelevante Informationen, z.B. Analyseergebnisse, nicht termingerecht bereit, müssen eventuell Besprechungen verschoben werden. Das hat negative Auswirkung auf Zeit und Verfügbarkeit der Beteiligten und auf die Fähigkeit zu zeitnahen, projektrelevanten Entscheidungen.

Verlust des Wettbewerbsvorsprungs

Die Grundlage für erfolgreiche Industriespionage und Produktpiraterie ist der unerlaubte aber mögliche Zugriff auf Informationen, die der Wettbewerb zu seinem Nutzen verwenden kann. Z.B. Skizzen, Konstruktionszeichnungen, Kalkulationen, Verträge, Analyseergebnisse, Prozessbeschreibungen, Patentinformationen, die den Wettbewerber durch Diebstahl von Daten von eigenen, aufwendigen Entwicklungstätigkeiten entlasten.

Reputationsschaden

Stellt sich heraus, dass Sie die Daten Ihrer Kunden nicht mit der gegebenen Sorgfalt verarbeitet oder ohne das Wissen Ihrer Kunden an andere Unternehmen weitergegeben haben, kann das Ihre Eignung zum Betrieb Ihres Geschäfts in Frage stellen. Beispiel: Kunden einer Bank können durch einen Fehler in der Online-Banking-Software die Konten anderer Kunden einsehen. Solche Ereignisse können Kunden dazu bringen, die Geschäftsbeziehung mit Ihnen abzubrechen und Behörden dazu veranlassen, Ihnen die Betriebserlaubnis zu entziehen.

Verstoß gegen gesetzliche Anforderungen

Insbesondere bei Projekten mit internationalem Kontext sind die unterschiedlichen Gesetzesvorgaben zum Umgang und zur Speicherung von Informationen zu beachten. Je nach Branche und Art der Organisation können Sie zur Weitergabe oder dem Schutz von Daten verpflichtet sein, die Ihren unternehmerischen Interessen gegebenenfalls gegenläufig sind oder bei Verstoß rechtliche Folgen haben. Achten Sie auch auf Meldepflichten gegenüber Behörden bei Informationssicherheitsvorfällen (z.B. KRITIS-Unternehmen gegenüber der Bundesnetzagentur).

Beendigung von Geschäftsbeziehungen & Schadenersatzforderungen aufgrund von Vertragsverletzungen

Sind Sie als Dienstleister in einem Projekt engagiert, unterliegen Sie vertraglich meist den kundenseitigen Anforderungen an Informationssicherheit. Der Verstoß gegen vertragliche Auflagen kann zu Schadenersatzforderungen bis hin zur Beendigung von Geschäftsbeziehungen führen.

Schützenswerte Informationen in Projekten

Welche Projektinformationen stehen damit im Fokus? Grundsätzlich können alle in einem Projekt benötigten und erstellten Informationen schützenswert sein. Um sie zu identifizieren, ihre Sensibilität zu bewerten und geeignete Schutzmaßnahmen ableiten zu können, ist es hilfreich, sie in Kategorien aufzuteilen. Die im Folgenden aufgeführten Kategorien machen zugleich deutlich, dass Informationssicherheit eine Querschnittsaufgabe ist, die alle Projektbeteiligten betrifft.

Projektmanagement-Informationen: "Managementprodukte"

Darunter sind alle Informationen zu verstehen, die relevant sind, um ein Projekt zu planen und zu steuern, Aufgaben zu managen, Produkte zu beschreiben und Entscheidungen zutreffen. Dies sind z.B.: Arbeitspaketbeschreibungen, Abnahmedokumente, Berichte, Pläne, Aufzeichnungen, Produktbeschreibungen u.s.w. PRINCE2 verwendet für diese Art von Informationen den Begriff "Managementprodukte". Managementprodukte können sowohl schriftlich dokumentiert vorliegen als auch mündlich formuliert sein.

Projektergebnisse: "Spezialistenprodukte"

Alle anderen im Rahmen des Projekts erzeugten Arbeitsergebnisse bezeichnet PRINCE2 als "Spezialistenprodukte" – diese zu erstellen ist der eigentliche Zweck eines Projekts. Diese Spezialistenprodukte, als Teil-, Neben- oder Gesamtergebnis der Projektarbeit (z.B. Skizzen, Konstruktionszeichnungen, Kalkulationen, Verträge, Analyseergebnisse, Prozessbeschreibungen, Patente), stellen einen hohen Wert dar, da sie gewissermaßen den im Projekt geschaffenen Informationsgewinn verkörpern. Sie sind dementsprechend bereits während des Projekts zu schützen. Gleiches gilt für alle Informationen über die Spezialistenprodukte.

Wettbewerbsrelevante Informationen

Dies sind Informationen, die relevant sind, damit das Unternehmen im Wettbewerb bestehen kann und die einen Marktvorsprung bedeuten oder Auswirkung auf marktregulierende Vorgänge haben. Dazu zählen z.B. Ergebnisse von Machbarkeitsstudien, Marktanalysen, Produktbeschreibungen in textueller und grafischer Form, Verträge oder Anträge auf Patente.

Informationen über die Projektorganisation

Informationen über Rollen, Verantwortlichkeiten, Personendaten (Organigramme, Rollenbeschreibungen, Personenverzeichnisse, Verzeichnisse zu Zugriffsrechten) sind besonders sensibel, da sie z.B. Ansatzpunkte für Angriffe auf die geschützten Informationen liefern können.

Informationen von Stakeholdern

Daten von Stakeholdern, insbesondere Kunden, die ausschließlich für die Verwendung im Projekt bereitgestellt werden (z.B. Produktionsdaten für Testzwecke, Personenverzeichnisse), sind besonders zu schützen, um Vertragsstrafen oder datenschutzrechtliche Folgen zu vermeiden.

Informationen, die Compliance-Anforderungen unterliegen

Auch aus subjektiver Sicht scheinbar "unkritische" Informationen können aufgrund bestehender Gesetze, Branchenstandards oder interner, selbst gesetzter Anforderungen besonderen Schutzanforderungen unterliegen. Dies betrifft insbesondere Prozessabläufe wie z.B. die Verarbeitung personenbezogener Daten im Rahmen von Integrations- und Abnahmetest. Es ist sicherzustellen, dass die Daten ausschließlich im Rahmen der vorab definierten Zwecke verwendet werden und z.B. Testprotokolle, die diese Daten enthalten, denselben Sicherheitsbestimmungen unterliegen wie die Originaldaten selbst.

Informationsträger: Technologien und Medien

Der beste Schutz für Informationen ist es, die Träger der Information vor unberechtigten Zugriffen und vor Beschädigungen zu schützen. Zur Aufbewahrung und Verarbeitung von schutzbedürftigen Projektinformationen werden immer mehr unterschiedliche Technologien und Medien verwendet wie z.B. Laptops, Mobiltelefone, Speichermedien aller Art, Projekt-Sharepoint, Notizbücher, Cloud-Speicher oder temporäre Kopien.

Sicherheitslücken in Projekten gefährden das Unternehmen

Genauso wie Einflüsse aus dem Umfeld die Informationssicherheit eines Projekts gefährden können, können auch aus einem Projekt Risiken für die Informationssicherheit in einer Organisation erwachsen. Anforderungen an die Informationssicherheit müssen deshalb auch projektübergreifende Aspekte berücksichtigen, um zu gewährleisten, dass Projekte und daraus hervorgehende Aktivitäten kein Risiko für die organisationsweite Informationssicherheit darstellen.

Zu den projektexternen, schützenswerten Informationen zählen z.B. für Testzwecke erforderliche Produktionsdaten, organisationsweite bzw. -übergreifende Personenverzeichnisse oder Schnittstellen zu projektexternen Datenverarbeitungsprozessen und -quellen. Diese für die Unternehmensorganisation wichtigen Informationen sind von den Projektverantwortlichen unabhängig von ihrer Bedeutung für das Projekt zu schützen.

Beispiel

Im Rahmen von Softwareprojekten in einer Bank, bei denen regelmäßig Software-Änderungen in die Produktionsumgebung zu überführen sind, werden explizite Zeiten (nur an Sonntagen, nur nachts etc.) für diese projektseitigen Rollouts vereinbart und auf Einhaltung überprüft.

Jedoch kann diese Anforderung der Informationssicherheit den Projektinteressen durchaus entgegenlaufen, da dies z.B. eine geringere Anzahl von Rollouts in einem Zeitrahmen zur Folge hat, Deployments für Ad-hoc-Korrekturen entfallen oder zusätzliche Personalkosten durch Nachtarbeit entstehen. Dieses Vorgehen schützt aber andere informationsverarbeitende Anlagen und -prozesse (z.B. Tagesendverarbeitungen im Bankenbereich) vor Störungen im Betriebsablauf, die weitaus größeren Schaden verursachen könnten, wie z.B. Reputations- und Finanzschaden durch fehlerhafte Buchungen, Produktions-Incidents mit Meldepflicht bei Behörden oder sogar Entzug der Betriebserlaubnis.

Informationssicherheit für Projekt und Organisation

Zusammenfassend sind daher bei der Implementierung eines Informationssicherheits-Managementsystems (ISMS) zwei Sichtweisen auf die Sicherheit von Projektinformationen zu berücksichtigen:

1. Interne Sicht: Gefahren für den Projekterfolg durch Vorfälle, welche die Sicherheit von Informationen gefährden.
2. Externe Sicht: Gefahren durch Vorfälle in Projekten, welche die Sicherheit von Informationen projektexterner Organisationen bedrohen.

Diese Informationswerte müssen mit Projektstart identifiziert und das Schutzniveau sowie Maßnahmen in Abhängigkeit von den Organisationsbedürfnissen definiert werden.

Informationssicherheit nach ISO 27001 und Projektmanagement

Die ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements (DIN 2013) ist die internationale Norm für das Management von Informationssicherheit. Sie wurde im Rahmen des deutschen Normierungsverfahrens übersetzt und steht nun auch auf Deutsch in Form der DIN ISO/IEC 27001:2017-06 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (DIN 2017) zur Verfügung.

Die ISO 27001 fordert in Anhang A, Abschnitt 5.1.5 (DIN 2017) ein, dass Informationssicherheit im Projektmanagement berücksichtigt wird, unabhängig von Art oder Branche des Projekts. Organisationen, die sich nach ISO 27001 zertifizieren lassen und Ihren angemessenen Umgang mit Informationen nachweisen möchten, müssen deshalb ebenfalls Projekte und Projektinformationen in ihre Betrachtungen einbeziehen.

Unterstützung dafür bieten z.B. die ISO 27002:2013 Information technology – Security techniques – Code of practice for information security controls (DIN 2016), die Maßnahmen zur Informationssicherheit vorschlägt oder das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI 2017), das unter anderem Lösungsvorschläge angepasst an die Bedürfnisse von kleinen, mittleren und großen Unternehmen bereithält.

Informationssicherheit im Sinne der ISO 27001

Die DIN ISO/IEC 27001:2017 (DIN 2017) stellt Mindestanforderungen und konkrete Maßnahmenziele an ein ISMS bereit, das durch den angemessenen Betrieb zur Informationssicherheit innerhalb einer Organisation beitragen soll. Im Wesentlichen bildet die Norm zwei Aspekte ab:

1. Mindestanforderungen an den Betrieb eines Managementsystems
2. Maßnahmenziele und Maßnahmen zur Förderung von Informationssicherheit verteilt auf 14 Themenbereiche

Mindestanforderungen an den Betrieb eines Managementsystems

Bei den Mindestanforderungen handelt es sich um sieben generisch formulierte Anforderungen zur Festlegung, Betrieb, Pflege und Verbesserung eines nachweisbaren ISMS unter Berücksichtigung der Anforderungen der Organisation hinsichtlich Informationssicherheit. Diese sind aus Sicht einer Zertifizierung nach ISO 27001 verbindlich und müssen vollständig umgesetzt werden. Diese sieben Kapitel der Norm werden getrieben durch den Anspruch an einen kontinuierlichen Verbesserungsprozess (Plan-Do-Check-Act = PDCA), die Fähigkeit zur Steuerung von Risiken (Risikomanagement) und die angemessene Umsetzung (Kontext der Organisation) mit branchenüblichen und zeitgemäßen Mitteln.

Organisation

Das ISMS ist am Kontext der Organisation auszurichten. Handelt es sich um ein Krankenhaus, eine Bank oder einen Produktionsbetrieb? Welche Informationen sind geschäftsrelevant? Abhängig davon, muss die Organisation in der Lage sein, die für sie relevanten Informationswerte und Interessengruppen zu bestimmen und angemessene Schutzmaßnahmen zu definieren. Im Bereich des Projektmanagements finden ähnliche Betrachtungen beim Erstellen des Business Cases statt.

Führung

Vorgaben zur Informationssicherheit gehen von der Geschäftsführung aus, die den Bezug zwischen IS und Geschäftserfolg erkennen und dokumentiert kommunizieren muss. Davon leiten sich grundlegende Vorgaben zu Anforderungen an die Informationssicherheit der Organisation ab, die auch im Projektmanagement zu berücksichtigen sind. "Führung" wird in Projekten durch den Lenkungsausschuss repräsentiert.

Planung

Hier geht es um die Planung der Maßnahmen zum Umgang mit Risiken, die Einfluss auf die Informationssicherheit haben. Voraussetzung dafür ist die Definition von Informationssicherheitszielen, die mit den Maßnahmen erreicht werden sollen. Auch im Projektmanagement gilt es, relevante Informationssicherheitsziele zu erkennen und diese bei der Projektplanung zu berücksichtigen.

Unterstützung

Der Betrieb eines ISMS bedarf geeigneter Ressourcen mit der notwendigen Kompetenz, um ihr Arbeitsfeld gemäß den Anforderungen an ein ISMS zu gestalten. Involvierte Personen müssen über ihre IS-Pflichten informiert und für das Thema IS sensibilisiert sein.

Betrieb

Die Umsetzung und Anpassung des ISMS muss auch im täglichen Betrieb gewährleistet sein. Dazu gehört, neue oder eingetretene IS-Risiken zu erkennen, zu melden, zu beurteilen und sie gemäß Risikobehandlungsplan zu managen.

Bewertung

Zu einem kontinuierlichen Verbesserungsprozess gehört auch eine regelmäßige Bewertung der erkannten IS-Risiken und der definierten Behandlungsmaßnahmen. Ziel ist es, anhand definierter Kennzahlen zu messen, in welchem Maß IS erreicht wird und bei Bedarf die definierten Maßnahmen anzupassen.

Verbesserung

Wurden mittels der Bewertungsaktivitäten Nichtkonformitäten im Bereich der Informationssicherheit erkannt, muss die Organisation angemessene Korrekturmaßnahmen ergreifen und dokumentieren. Die Wirksamkeit der ergriffenen Maßnahmen muss im Rahmen des ISMS-Betriebs beobachtet, geprüft und bewertet werden und kann ggf. weitere Korrekturen zur Folge haben.

14 Organisationsbereiche zur Betrachtung von Informationssicherheit

Im Blickpunkt der Norm stehen 14 wesentliche Bereiche in Organisationen, in denen Informationswerte eine Rolle spielen, und die Maßnahmen zum systematischen Umgang mit den daraus resultierenden Risiken. Innerhalb dieser 14 Bereiche formuliert die Norm konkrete Maßnahmenziele und Maßnahmen, die Sie bei der Umsetzung eines ISMS heranziehen sollten, insbesondere, wenn Sie eine Zertifizierung nach ISO 27001 anstreben. Diese sind in Anhang A der Norm aufgeführt. Die 14 Organisationsbereiche und ihre Bedeutung für die IS sind im Folgenden kurz vorgestellt (die Bereiche "Zugriff" und "Verschlüsselung" sowie "Störungen" und "Kontinuität" sind jeweils zusammengefasst).

Leitlinien

Die Norm geht davon aus, dass die Leitung einer Organisation ihre unternehmenskritischen Informationen sowie die damit verbundenen Risiken kennt und daraus dokumentierte Anforderungen an den sicheren Umgang mit Informationen ableitet.

Personal(-sicherheit)

Die Mitarbeiter einer Organisation verwenden Informationen, um Aufgaben zu erfüllen. Damit der angemessene Umgang mit diesen Informationen sichergestellt ist, müssen alle Mitarbeiter über die organisationseigenen Leitlinien zum Umgang mit internen Informationen aufgeklärt werden. Die Organisation ist auch verpflichtet, die persönliche Eignung ihrer Mitarbeiter für den Umgang mit schützenswerten Informationen festzustellen.

Externe Dienstleister

Häufig benötigen externe Lieferanten Zugriff auf unternehmenseigene Informationen, um im Sinne der Organisation Dienstleistungen erbringen zu können. Es muss sichergestellt werden, dass dabei die geltenden Anforderungen an die Informationssicherheit wirksam berücksichtigt werden.

Organisation

Leitung, Personal und externe Lieferanten ergeben eine über Rollen und Verantwortlichkeiten definierte und strukturierte Organisation mit verschiedenen Interessengruppen, die sich in ihren Informationsbedürfnissen unterscheiden. Innerhalb dieser Organisation muss die Verantwortung für das ISMS geklärt sein. Das gilt auch für Projekte.

Werte / Assets

Die Informationen und deren Speicher- und Verarbeitungsmedien ergeben aus Sicht der Informationssicherheit die zu schützenden Werte der Organisation und sind die Grundlage für die Betrachtung von Informationssicherheits-Maßnahmen

Kommunikation

Das Personal verarbeitet im Rahmen seiner Verantwortlichkeiten vorhandene Informationen entlang der gegebenen Organisationsstruktur und greift dafür über Speicher- und Verarbeitungsmedien oder in mündlicher Form auf Informationen zurück. Diese Form der Kommunikation muss aufrechterhalten, aber auch gesteuert werden, z.B. durch die Beschränkung von Zugriffen auf Informationen und durch damit einhergehende Rechte- und Rollenkonzepte.

Zugriff und Verschlüsselung

Mittel zur Sicherstellung von Informationssicherheit sind Zugriffs- und Verschlüsselungsstrategien, die verhindern sollen, dass Unbefugte Zugang zu Informationsträgern und verarbeitenden Einrichtungen erhalten. Verschlüsselung hilft, das Auslesen der Daten zu verhindern, selbst wenn ein unberechtigter Zugang zu Informationsträgern erfolgt.

Betrieb

Der Schutz von Informationen und deren verarbeitenden oder speichernden Medien muss im laufenden Betrieb gewährleistet werden, indem die in der Organisationsstruktur definierten Verantwortlichkeiten wahrgenommen werden. Umgekehrt sind Informationen notwendig, um den Betrieb zu ermöglichen.

Entwicklung

Im Rahmen der Weiterentwicklung von informationsverarbeitenden Systemen müssen die Anforderungen an die Sicherheit von Informationen und deren Systeme berücksichtigt werden.

Physische Bedrohungen / Umwelt

Aus dem Umfeld von Organisationen können sich vielfältige Gefahren (Diebstahl, Wasserschäden, Beschädigung) für Informationswerte ergeben. Diese müssen im Rahmen von Risikobetrachtungen analysiert, im Betrieb berücksichtigt und geeignete Schutzmaßnahmen implementiert werden.

Compliance

Neben selbst auferlegten Anforderungen an die Informationssicherheit muss eine Organisation auch die für ihre Branche oder aufgrund von Gesetzeslagen geltenden Anforderungen mit Einfluss auf die Informationssicherheit kennen und bei der Definition ihres Schutzniveaus berücksichtigen.

Störungen und Kontinuität

Sollte es doch einmal zu Störungen kommen, müssen vorab definierte Maßnahmen und Prozesse zur Behebung eingeleitet werden, um das erwartete Informationssicherheitsniveau im Sinne eines kontrollierten Kontinuitäts-managements wiederherzustellen.

Integration von Managementsystemen

Bei PRINCE2® und anderen Projektmanagement-Ansätzen mit ausgeprägter Orientierung am PDCA-Zyklus sowie bei der ISO 27001 als Standard für die Informationssicherheit handelt es sich um systemische Ansätze, mit sich überschneidenden Anforderungen zur Steuerung des jeweiligen Umfelds. Dazu gehören unter anderem Themen wie Qualitätsmanagement, Risikomanagement, Änderungsmanagement, Planung und Verbesserungsprozesse.

Es ist deshalb naheliegend, die beiden Managementsysteme für Informationssicherheit und Projektmanagement zu kombinieren, um den Overhead insgesamt gering zu halten. Auch die ISO 27001:2017 fordert in Kap. 0.1, Abs. 3 die Integration in die Ablauforganisation: "Es ist wichtig, dass das Informationssicherheitsmanagementsystem als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt wird." (DIN 2017).

Die Integration des ISMS in das PMS soll die Wirksamkeit beider Managementsysteme erhöhen, d.h. Aufwände (Ressourcen, Kosten, Zeit) reduzieren und den Nutzen erhöhen. Dies kann unter anderem durch folgende Effekte erreicht werden:

- Keine Doppelarbeiten durch parallele Managementsysteme
- Vereinfachung durch Standardisierung von Verfahren und Dokumenten
- Reduktion des organisatorischen Overheads durch Integration in bestehende Rollenkonzepte
- Zusammenlegung von Audits
- Identifizierung und Optimierung von Schnittstellen zwischen den Managementsystemen

- Vermeidung von Reibungsverlusten zwischen den Managementsystemen, indem konträre Regelungen und Zielkonflikte identifiziert und aufgelöst werden
- Erhöhung der Akzeptanz bei den Mitarbeitern, z.B. durch möglichst geringe Veränderungen an etablierten Verfahren

Ein möglicher Integrationsansatz für Managementsysteme

Jede Organisation hat ein "Managementsystem" (MS), d.h. ein systematisches Vorgehen mit wiederkehrenden Arbeitsweisen, um bestimmte Problemstellungen zu lösen. Aber: Ein Verfahren kommt selten allein – d.h. es sind mehrere Managementsysteme notwendig, die sich überschneiden oder sogar umschließen. Beispiel: Ein Projektmanagementsystem enthält Aspekte wie Qualitätsmanagement, Risikomanagement, Verbesserungs- und Änderungssteuerungsverfahren. Es überschneidet sich damit u.a. mit dem Qualitätsmanagementsystem und dem Risikomanagementsystem.

Managementsysteme oder Verfahren lassen sich einzeln, in Teilen oder in Verbindung mit anderen Verfahrensbausteinen in Unternehmen bzw. Organisationen betreiben. Aber wäre es nicht effizienter, wenn Sie für all Ihre Verfahren z.B. ein einheitliches Risikomanagementverfahren nutzen würden? Hierzu müssen Sie die Managementsysteme miteinander verbinden. Werden getrennte Managementsysteme zu einem einheitlichen Managementsystem verbunden, spricht man von einem integrierten Managementsystem (IMS).

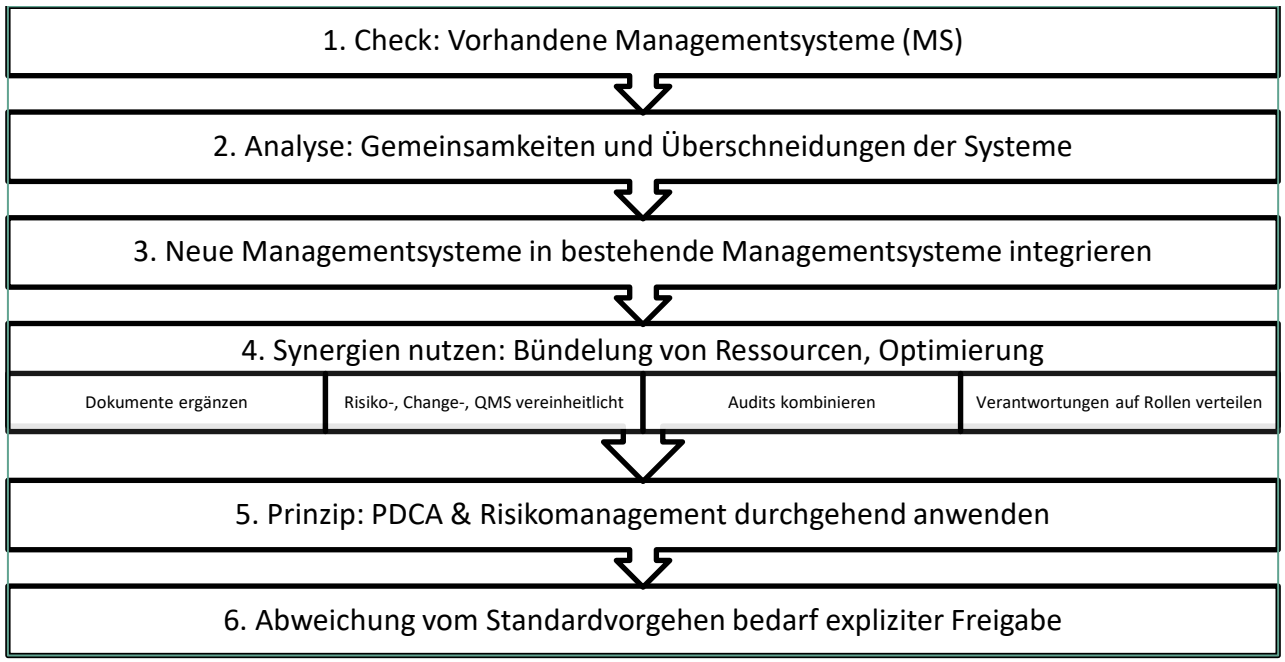

Bild 1: Integrationsansatz für Managementsysteme

Die Integration des Informationssicherheitsmanagements in das Projektmanagement erfordert somit ein Vorgehen, für das ich im Folgenden einen grundsätzlichen Vorschlag vorstelle (Bild 1). Als Beispiel für eine solche Integration

finden Sie im Anhang ausführliche Hinweise, wie die Anforderungen der ISO 27001 in das PMS PRINCE2 eingearbeitet werden können. Dieses Vorgehen funktioniert natürlich auch für Projektmanagementansätze, die nicht auf PRINCE2 basieren, aber grundsätzlich systemische Ansätze verfolgen.

1. Check: vorhandene Managementsysteme (MS)

Im ersten Schritt überlegen Sie sich, welche Managementsysteme und Arbeitsrichtlinien in der Organisation bereits vorhanden sind. Gibt es schon Verfahren für Change Management oder Risikomanagement? Liegen Projektmanagement- oder Qualitätsmanagement-Handbücher vor, die Sie für Ihre Betrachtungen heranziehen können? Erstellen Sie eine Übersicht dieser Verfahren und Ihrer Dokumentationen.

2. Analyse der Gemeinsamkeiten und Überschneidungen der Systeme

Schauen Sie sich die aufgelisteten Verfahrensbeschreibungen im Hinblick auf Gemeinsamkeiten und Überschneidungen genauer an. Wo könnten Teilsysteme vernetzt werden?

Sie werden feststellen, dass es in Ihrer Organisation Prozesse gibt, die sich schon aus thematischen Gründen nicht zusammenlegen lassen. Hierfür gilt es dann, eigenständige Vereinbarungen für den Umgang mit diesen Themen zu treffen.

Erweitern Sie ihre Liste, ausgehend vom zu integrierenden System (z.B. ISMS), auf vorhandene und noch nicht vorhandene Elemente. Das vorhandene Qualitätsmanagement-Handbuch z.B. liefert ein Verfahren zum Management von Qualität und die Sicherstellung eines PDCA-Zyklus, aber keinen Risikomanagementansatz wie für ein ISMS benötigt.

3. Neue Managementsysteme in bestehende Managementsysteme integrieren

Schauen Sie sich die vorhandenen Elemente nun im Detail an. Überlegen Sie sich in diesem Schritt, welche Komponenten aus vorhandenen Systemen nur um Aspekte der Informationssicherheit erweitert, aber nicht neu definiert werden müssten. Kann der Risikomanagementansatz z.B. um die Risikokategorie "Informationssicherheit" erweitert werden? Kann das Change Management zukünftig auch Aspekte der Informationssicherheit berücksichtigen?

Schauen Sie sich dann die Elemente an, die in Ihren vorhandenen Verfahrensanweisungen noch nicht beschrieben sind. Entwickeln Sie hierfür neue Lösungsansätze und dokumentieren Sie das Verfahren.

4. Synergien nutzen: Bündelung von Ressourcen, Optimierung

Effizienzsteigerung ist ein Ziel beim Betrieb integrierter Managementsysteme. Hierfür ist die Nutzung von Synergien und die Bündelung von Ressourcen wichtig. Prüfen Sie, ob bestehende Dokumente um neue Anforderungen ergänzt werden können, statt neue Dokumente zu erstellen. Vereinheitlichen Sie, falls notwendig und möglich, vorhandene Ansätze und Anforderungen an typische Systemthemen wie Risiko-, Change- und Qualitätsmanagement. Audits können kombiniert und Verantwortungen, die sich aus dem neuen Managementsystem ergeben, auf bestehende Rollen verteilt werden.

5. Prinzip: PDCA & Risikomanagement durchgehend anwenden

Systemische Managementansätze leben vom Prinzip der "kontinuierlichen Verbesserung" (PDCA) in Kombination mit einer durchgehenden Risikobetrachtung. Achten Sie daher darauf, dass dies im Rahmen Ihres integrierten Ansatzes für alle vernetzten Systeme immer noch möglich ist.

6. Abweichung vom Standardvorgehen bedarf expliziter Freigabe

Gilt ein integriertes und vereinheitlichtes Managementsystem für die gesamte Organisation, darf nicht ohne weiteres ein anderes Managementsystem eingesetzt werden, das nicht dem Organisationsstandard entspricht, da dies zu Effizienzverlusten führen würde. Die Verwendung eines anderen Managementsystems bedarf der Rechtfertigung gegenüber dem Topmanagement und dessen expliziter Freigabe.

Integrieren Sie Informationssicherheit in Ihr Projektmanagementsystem!

Warum also Informationssicherheit auch im Projektmanagement berücksichtigen? Was ist bei der Implementierung eines integrierten Informationssicherheitssystems zu beachten? Mit den folgenden sieben Handlungsempfehlungen und Appellen möchte ich Sie motivieren, konkrete Schritte in Richtung einer sicheren digitalen Zukunft zu gehen.

Kennen Sie Ihren Wert!

Machen Sie sich bewusst, welche Bedeutung Informationswerte für Ihren Organisationserfolg haben. Was sind Ihre Informationswerte? Was bedeutet deren Verlust, Nichtverfügbarkeit oder Beschädigung für Ihren Unternehmens- und Projekterfolg?

Ein Projekt ist so sicher, wie Sie es machen!

Sie selbst bestimmen Umfang und Schutzniveau für die Informationssicherheit in Ihrer Organisation und zugehöriger Projekte!

Schaffen Sie eine solide Basis!

Berücksichtigen Sie Informationssicherheitsanforderungen von Projektbeginn an in Ihren Projektmanagement-aktivitäten und bei der Aufstellung der Projektorganisation.

Skalieren Sie!

Stimmen Sie den Umfang der Maßnahmen auf Projektgröße und -umfang ab. Betreiben Sie wenn möglich integrierte Managementsysteme.

Keiner ist allein!

Berücksichtigen Sie bei der Analyse Ihres Sicherheitsbedarfs auch die Auswirkungen der Projektaktivtäten auf die organisationsweite und organisationsexterne Informationssicherheit.

Seien Sie konsequent!

Berücksichtigen Sie Informationssicherheit in allen Phasen eines Projekts und teilen Sie Ihre Erfahrungen.

Profitieren Sie von Ihren bestehenden Managementsystemen!

Verhindern Sie Doppelaufwände für die Einführung eines ISMS durch die Nutzung und Integration in Ihre bestehenden Systeme. Wie das konkret für ein Projektmanagementsystem erfolgen kann, erfahren Sie im beigefügten Umsetzungsbeispiel: "Integration der ISO 27001 in PRINCE2®".

Literatur

- AXELOS (Hrsg.): Managing Successful Projects with PRINCE2, 6th ed., UK, The Stationery Office Ltd TSO, 2017
- BMJV Bundesministeriums der Justiz und für Verbraucherschutz: Das Energiewirtschaftsgesetz, 31 08 2017, https://www.gesetze-im-internet.de/enwg_2005/EnWG.pdf (Zugriff am 11 02 2018)
- BSI Bundesamt für Sicherheit in der Informationstechnik: Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen, 2016 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=6 (Zugriff am 11 02 2018)
- BSI Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html (Zugriff am 01 Mai 2017)
- DIN Deutsches Institut für Normung e. V.: DIN ISO/IEC 27001:2013, Berlin, Beuth Verlag GmbH, 2013
- DIN Deutsches Institut für Normung e.V.: DIN ISO/IEC 27001:2015-03 Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen, Bd. ISO/IEC 27001:2013 + Cor. 1:2014, Berlin, Beuth Verlag GmbH, 2015-03
- DIN Deutsches Institut für Normung e.V.: DIN ISO/IEC 27002:2016-11 Informationstechnologie - IT-Sicherheitsverfahren - Leitfaden für Informationssicherheits-Maßnahmen, Bd. (ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015), Berlin: Beuth Verlag GmbH, 2016-11
- DIN Deutsches Institut für Normung e. V.: DIN EN ISO/IEC 27001:2017-06 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)., Berlin, Beuth Verlag GmbH, 2017

Hat Ihnen dieser Artikel gefallen?

Bewerten Sie ihn im Projekt Magazin online und teilen Sie so Ihre Meinung anderen Lesern mit. Wählen Sie dazu den Artikel im Internet unter https://www.projektmagazin.de/ausgaben/2018 oder klicken Sie hier, um direkt zum Artikel zu gelangen.