Umsetzungsbeispiel zum Artikel:
Informationssicherheit im Projekt nach ISO 27001 mit PRINCE2©

Integration der ISO 27001 in PRINCE2®

von Stefanie Eilhardt

Informationssicherheitsmanagement ist eine Querschnittsaufgabe, die alle Bereiche eines Projektmanagement-systems (PMS) beeinflusst. Im Folgenden finden Sie Beispiele und Anregungen, wie Sie die Anforderungen eines Informationssicherheits-Managementsystems (ISMS) in Ihrem PMS umsetzen können. Dies geschieht beispielhaft und ohne Anspruch auf Vollständigkeit am international weit verbreiteten Standard PRINCE2®. Vieles davon können Sie direkt auf andere PMS übertragen. Einige Aspekte sind spezifisch für PRINCE2, insbesondere die Schnittstellen zum Projektumfeld, die z.T. in anderen PMS nicht berücksichtigt werden. Hier ist ggf. eine Erweiterung des betrachteten PMS erforderlich.

Die Darstellung folgt der im Handbuch (AXELOS 2017, S. 3) präsentierten Struktur von PRINCE2®. Daraus resultieren zwar einige Redundanzen, aber Sie können dadurch den Vorschlägen schnell die jeweiligen Abschnitte im Handbuch zuordnen. Die sog. "vier integrierten Elemente" von PRINCE2 sind:

- Prinzipien
- Themen
- Prozesse
- Projektumfeld

Insbesondere im Rahmen der Projektmanagement-Prozesse, aber auch bei den Prinzipien, beschreibe ich zudem die Bedeutung einzelner sog. Managementprodukte (dies sind bei PRINCE2 alle Dokumente des Projektmanagements) für das ISMS. Zur einfachen Erkennung sind die von PRINCE2 definierten Managementprodukte kursiv dargestellt, z.B.: *Business Case*. Die Aufgaben einiger von PRINCE2 definierten Rollen für die Informationssicherheit stelle ich beim Prinzip "Definierte Rollen und Verantwortlichkeiten" sowie bei einigen Prozessschritten vor.

Prinzipien

Mit der Formulierung von sieben Prinzipien definiert PRINCE2 zentrale Verhaltensgrundsätze für das Managen eines Projekts. Diese Grundsätze prägen alle Projektmanagement-Prozesse und Themen und sind somit auch auf Aspekte der Informationssicherheit (IS) anzuwenden. Die sieben Prinzipien sind gleichberechtigt und müssen alle erfüllt sein, damit ein Projektmanagementsystem konform mit PRINCE2 ist.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Prinzip	Deutsche Übersetzung
Continued business justification	Fortlaufende geschäftliche Rechtfertigung
Learn from experience	Lernen aus Erfahrungen
Defined roles and responsibilities	Definierte Rollen und Verantwortlichkeiten
Manage by stages	Steuern über Managementphasen
Manage by exception	Steuern nach dem Ausnahmeprinzip
Focus on products	Produktorientierung
Tailor to suit the project	Anpassen an die Projektumgebung

Tabelle 1: Die sieben Prinzipien von PRINCE2

Andere PMS formulieren nicht explizit ihre Prinzipien, auch erheben die sieben Prinzipien von PRINCE2 nicht den Anspruch auf Vollständigkeit. Vorteil der Prinzipien ist, dass sie in sehr komprimierter Form einen allgemeinen Rahmen für das Managen von Projekten in einer professionellen Umgebung beschreiben.

Fortlaufende geschäftliche Rechtfertigung

Dieses Prinzip fordert, dass für jedes Projekt der daraus erwartete geschäftliche Nutzen dokumentiert, vom Lenkungsausschuss genehmigt und zu jedem Phasenübergang überprüft wird.

Im Einklang dazu besteht die ISO 27001 (DIN 2017) auf regelmäßigen Beurteilungen der Risiken für die Informationssicherheit. Hierbei ist das Schutzniveau für Organisationsdaten unter Berücksichtigung der Geschäftsziele auf ihre Angemessenheit hin zu prüfen, dokumentiert zu bestätigen bzw. zu revidieren.

Der Projektmanager hat deshalb zusammen mit der geschäftlichen Rechtfertigung zu prüfen: Steht das für das Projekt relevante Schutzniveau für Informationen noch in gesunder Relation zu den auf das Projekt wirkenden oder aus dem Projekt entstehenden Risiken? Um diese Frage zu beantworten, wertet er das *Risikoregister*, evtl. vorhandene *Ausnahmeberichte* und die *Phasenabschlussberichte* aus. So erhält der Projektmanager Indikatoren dafür, ob eine Häufung von IS-Vorfällen mit Handlungsbedarf vorliegt.

Beispiel: Bei einer Bank verursachten im Rahmen eines Software-Entwicklungsprojekts durchgeführte unternehmensweite Rollouts von Updates Störungen im Betrieb der produktiven Online-Banking-Plattform. Diese erforderten aufwendige Korrekturen und führten zum Ausfall der Online-Banking-Services, was auch den Kunden nicht verborgen blieb.

In diesem Beispiel bewirkten die Projektaktivitäten Sicherheitsvorfälle im Unternehmen, die dessen Erfolg gefährdeten (Verlust von Renommee, Kosten für Korrekturen, Schadensersatzforderungen). Dementsprechend mussten die im Projekt verwendeten Verfahren (regelmäßige unternehmensweite Rollouts) überprüft und angepasst werden. Dabei war auch zu prüfen, ob das IS-Risiko, das aus dem Betrieb des Projekts entsteht, dessen Weiterführung rechtfertigt. Stehen die Kosten für die Lösung von IS-Vorfällen oder die Risikobehandlung noch in angemessenem Verhältnis zum

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

erwarteten Projektnutzen? Der Projektverantwortliche muss, ggf. auch unter Einbeziehung des IS-Verantwortlichen und des Lenkungsausschusses, über die notwendigen Maßnahmen entscheiden und diese im Sinne eines nachvollziehbaren Steuerungs-Prozesses (Plan-Do-Check-Act) dokumentieren.

Lernen aus Erfahrung

Mit diesem Prinzip gewährleistet PRINCE2 einen kontinuierlichen Verbesserungsprozess nicht nur hinsichtlich des Projektgegenstands, sondern auch für das PMS selbst.

Gleichermaßen sollte der Projektmanager deshalb auch Erfahrungen hinsichtlich Informationssicherheit berücksichtigen, im *Erfahrungsprotokoll* dokumentieren und nachfolgenden Projekten mit dem *Erfahrungsbericht* zur Verfügung stellen. Empfehlungen können ausgesprochen werden an die Verantwortlichen für den Betrieb des unternehmensweiten ISMS, zur Optimierung von Schnittstellen zwischen Projektmanagement und Informationssicherheit im Betrieb.

Definierte Rollen und Verantwortlichkeiten

Grundlage für eine effiziente Projektsteuerung ist eine Organisationsstruktur mit definierten Rollen und Verantwortlichkeiten, die regelt, welche Rechte und Pflichten eine Rolle im Rahmen des Projektmanagements übernimmt. PRINCE2 stellt hierzu sein Organisationsmodell (s.u. Thema "Organisation") und eine Reihe von Vorlagen für Rollenbeschreibungen zur Verfügung.

Die Rollenbeschreibungen definieren unter anderem die Befugnisse und Verantwortungen der Rolle. Erweitert auf Aspekte der Informationssicherheit sollten sie somit auch regeln:

- Wer für das Thema "Informationssicherheit" im Projekt verantwortlich ist und bei Informationssicherheitsvorfällen haftet.
- Welche Informationswerte es im Projekt gibt und welche Rollen und Verantwortlichkeiten sich daraus für welche Rolle ergeben.
- Den Zugriff auf Informationswerte: Wer darf und muss wann was wissen, um seine Aufgaben zu erfüllen? Wer sendet? Wer empfängt? Wer sollte vom Empfang welcher Information ausgeschlossen werden?
- Wie die Inhaber von Rollen über ihre Verantwortlichkeiten und Befugnisse hinsichtlich Informationssicherheit informiert werden und wie dies nachweisbar dokumentiert wird (unterzeichnete Stellen- und Rollenbeschreibungen, Aufzeichnungen über Schulungen).
- Wie überprüft wird, dass dem Verantwortlichen seine Rolle für die Informationssicherheit bekannt ist und er dementsprechend handelt (Audits).

Für zentrale Rollen im Projektmanagementteam zeige ich im Folgenden mögliche Umsetzungsbeispiele für die Zuweisung von IS-Verantwortlichkeiten in ihren Rollenbeschreibungen auf.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Lenkungsausschuss

Diese Rolle stellt für das Projekt die Verbindung zur Geschäftsführung (oder zum Programm-Management) dar. Sie hat sicherzustellen, dass die für das Projekt relevanten Anforderungen aus dem organisationsweiten ISMS (Informationssicherheitspolitik, Informationssicherheitsziele) auch im Projekt bekannt sind und durch Zuweisungen von Rollen und Verantwortlichkeiten in der Projektarbeit berücksichtigt werden.

Umsetzungsbeispiel: Der Lenkungsausschuss informiert den Projektmanager über die hohe Kritikalitätsstufe des Projekts und das erwartete Informationssicherheitsniveau. Er fordert ein, dass alle Informationen zum Projekt vertraulich behandelt werden müssen und ausschließlich organisationsintern einem dafür definierten Personenkreis zugänglich gemacht werden dürfen. Er fordert den Projektmanager auf, geeignete Maßnahmen zu ergreifen, um dies im Projekt sicherzustellen.

Projektmanager

Diese Rolle berücksichtigt Vorgaben zur Informationssicherheit im Tagesgeschäft und stellt sicher, dass das Projekt die geforderten Produkte erstellt innerhalb der für die Informationssicherheit gesetzten Toleranzen (bezüglich Zeit, Kosten, Qualität, Umfang, Risiko und Nutzen). Er erkennt Informationssicherheitsrisiken im Rahmen der Wahrnehmung seiner Risikomanagementaufgaben. Für diese entwickelt und implementiert er geeignete Lösungen.

Umsetzungsbeispiel: Der Projektmanager informiert das Projektteam über die besonderen Vertraulichkeitsanforderungen. Als Maßnahme stellt er beispielsweise sicher, dass mündliche wie fernmündliche Projektgespräche und Meetings in abhörsicheren Räumlichkeiten wie Konferenzräumen stattfinden. Dokumente werden ausschließlich über interne E-Mail- und Telekommunikation mit dem erforderlichen Vertraulichkeits-Vermerk versandt. Projektdokumente werden nicht auf dem privaten Laufwerk gespeichert, sondern im geschützten Projektbereich auf dem internen Projektlaufwerk. Dies stellt sicher, dass alle berechtigten Rollen bei Bedarf auf das Arbeitsergebnis zugreifen können (Nutzen) und ein geeigneter Sicherungsgrad (Qualität) hinsichtlich Backup, Archivierung und Zugriffschutz eingehalten wird. Doppelaufwände (Zeit- und Kostenaufwand) für die Erstellung oder das Auffinden von nicht abrufbaren oder verlorenen Dokumenten werden vermieden.

Teammanager

Diese Rolle berücksichtigt bei der Erstellung der Spezialistenprodukte ebenfalls die Vorgaben, wie mit den Produkten und den damit verbundenen Informationen umzugehen ist. Er stellt sicher, dass der erforderliche Vertraulichkeitsgrad auf seiner Ebene angemessen umgesetzt wird. Abweichungen werden an den Projektmanager kommuniziert.

Umsetzungsbeispiel: Der Teammanager erhält vom Projektmanager Informationen über die besonderen Vertraulichkeitsanforderungen und daraus abgeleiteten Sicherungsmaßnahmen. Der Teammanager informiert sein Team und stellt sicher, dass bei der Produkterstellung und gegebenenfalls darüber hinaus unter den vom Projektmanager benannten Bedingungen gearbeitet wird. Er identifiziert die mit einem *Arbeitspaket* auf seiner Ebene verbundenen Risiken und offenen Punkte, meldet diese dem Projektmanager und empfiehlt Maßnahmen zur Risikobehandlung.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Projektsicherung

Diese vom Lenkungsausschuss delegierbare Rolle gewährleistet die Wahrnehmung der Interessen der wichtigsten Stakeholder (Lenkungsausschuss, externe Parteien). Diese Aufgaben können nicht an den Projektmanager übertragen werden. Liegen Informationssicherheitsanforderungen an das Projekt vor, kann die Projektsicherung den Lenkungsausschuss bei der Überprüfung ihrer Einhaltung unterstützen. Dafür müssen die zu schützenden Informationswerte und das Schutzniveau definiert und bekannt sein. Stellt die Projektsicherung Nachbesserungsbedarf im Bereich der Informationssicherheit fest, muss diese Rolle auch sicherstellen, dass die beschlossenen Maßnahmen ordnungsgemäß implementiert werden.

Umsetzungsbeispiel: Mitarbeiter der Projektsicherung prüfen im Rahmen der regulären Projektmanagementaudits auch Anforderungen an die Informationssicherheit. Sie entnehmen der *Projektleitdokumentation* die dokumentierten Sicherheitsanforderungen und erhalten beim Projektleiter Auskunft über die ergriffenen Maßnahmen. Die Projektsicherung beurteilt die Angemessenheit und korrekte Umsetzung der Maßnahmen, z.B. anhand von Stichproben an Dokumenten und Sicherheitsstufen auf dem Projektlaufwerk, tatsächlichen Vertraulichkeitskennzeichnungen in versendeten E-Mails und Rauminformationen aus den Meeting-Protokollen.

Projektunterstützung

Diese Rolle, auch als Projektunterstützung oder Project Office bekannt, kann den Projektmanager bei der Einrichtung und dem administrativen Betrieb des Informationssicherheits-Managementsystems beraten und unterstützen. Möglicherweise fällt dies auch in den Aufgabenbereich eines PMO.

Umsetzungsbeispiel: Auch die Mitarbeiter der Projektunterstützung müssen vom Projektmanager über die besonderen Vertraulichkeitsanforderungen an das Projekt informiert werden. Die Projektunterstützung kann das Dokumentenmanagement und den Betrieb des Projektlaufwerks übernehmen. Sie hilft bei der Beschaffung entsprechender Räumlichkeiten und zugehöriger Infrastrukturen. Diese Rolle unterstützt mit administrativer Vorbereitung und Zuarbeiten die Tätigkeit der Projektsicherung (Audit-Unterstützung).

Steuern über Managementphasen

Informationssicherheit muss sorgfältig geplant, überwacht und gesteuert werden. Aufgrund der Steuerung über Managementphasen weist ein PRINCE2-Projekt definierte Phasenbewertungen und Freigaben an den Phasenübergängen auf. Diese Phasenabnahmen und das kontrollierte Abschließen eines Projekts sind prädestinierte Kontrollpunkte, um auch Sicherheitsanforderungen zu berücksichtigen.

Steuern nach dem Ausnahmeprinzip

Als Teil der Projektbeschreibung haben Sie Toleranzen für Informationssicherheit (s.o. Rollenbeschreibung Projektmanager) definiert und in Abstimmung mit dem Lenkungsausschuss vereinbart. Nur wenn diese Toleranzen absehbar überschritten werden oder sich definierte IS-Steuerungsmittel als nicht angemessen erweisen, ist es erforderlich, den Lenkungsausschuss in Form eines *Ausnahmeberichts* zu unterrichten und von ihm entsprechende Unterstützung anzufordern, z.B. durch Genehmigung weiterer, sicherheitsrelevanter Maßnahmen.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Definieren Sie im Rahmen der Toleranzbestimmung auch Toleranzen für IS-Vorfälle. Wann ist der Lenkungsausschuss zu benachrichtigen? Im Rahmen des *Kommunikationsmanagement-Ansatzes* legen Sie fest, welche IS-Risiken an wen zu welchem Zeitpunkt berichtet werden müssen.

Produktorientierung

Die Ergebnisorientierung in einem Projekt kommt Ihnen auch bei der Steuerung der Informationssicherheit entgegen. Beziehen Sie die für ein angemessenes Sicherheitsniveau benötigten Produkte (z.B. ein verschlüsselter und zugangsgeschützter Datenspeicher) bei der produktbasierten Planung mit ein. Überprüfen Sie diese Produkte, ob sie gemäß den dafür definierten Qualitätsanforderungen aus dem *Qualitätsmanagement-Ansatz* geeignet sind, das Ziel zu erreichen.

Anpassen an die Projektumgebung

So wie das Projektmanagementsystem und seine Steuerungsmittel an die Projekt- und Unternehmensbedürfnisse angepasst werden sollen, so fordert auch die ISO 27001 zu einem angemessenen Einsatz der Mittel auf. Auch beim ISMS gilt: Beim Anpassen an Projekt und Projektumfeld wird nichts weggelassen, sondern zielorientiert skaliert! Kurze Handlungsempfehlungen finden Sie bei der Beschreibung des Elements "Projektumgebung" (s.u.).

PRINCE2-Themen

Die sieben Themen von PRINCE2 (bzw. Wissensbereiche) stellen eine wichtige Schnittstelle zu den Mindestanforderungen an den Betrieb eines Managementsystems dar, wie sie in der ISO 27001 gefordert werden (siehe hierzu: Informationssicherheit im Projekt nach ISO 27001 mit PRINCE2©, Projekt Magazin, 08/2018). Sie sind wichtig für den systematischen Betrieb von Informationssicherheit. Hier ergeben sich etliche Überschneidungen, die für den erfolgreichen Aufbau und die effiziente Integration von Informationssicherheitsmanagement in ein PMS verwendet werden können.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

ISO 27001	PRINCE2			
Mindestanforderungen	***Themen***	***Prinzipien***	***Techniken***	***Managementansätze***
Kontext der Organisation	Business Case	Fortlaufende geschäftliche Rechtfertigung		Managementansätze für Qualität, Risiko und Kommunikation, Änderungssteuerungsansatz
Führung	Organisation	Steuern über Managementphasen		Managementansätze für Qualität, Risiko und Kommunikation, Änderungssteuerungsansatz
Planung	Pläne, Qualität, Risikomanagement	Definierte Rollen und Verantwortlichkeiten	Produktbasierte Planung	Managementansätze für Qualität, Risiko und Kommunikation, Änderungssteuerungsansatz
Unterstützung	Organisation	Definierte Rollen und Verantwortlichkeiten		
Betrieb	Risikomanagement	Steuern nach dem Ausnahmeprinzip		Risikomanagement-ansatz
Bewertung der Leistung	Qualität (PDCA); Risikomanagement	Produktorientierung	Qualitätsprüfungstechnik	Qualitätsmanagementansatz, Risikomanagementansatz
Verbesserung	Fortschritt, Qualität; Risikomanagement	Lernen aus Erfahrungen		Qualitätsmanagementansatz, Risikomanagementansatz
Themenbereiche (IS-Ziele)				
Informationssicherheitsrichtlinien	Business Case			Managementansätze für Qualität, Risiko und Kommunikation, Änderungssteuerungsansatz
Organisation der Informationssicherheit	Organisation	Definierte Rollen und Verantwortlichkeiten		Managementansätze für Qualität, Risiko und Kommunikation, Änderungssteuerungsansatz
Personalsicherheit		Definierte Rollen und Verantwortlichkeiten		

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

ISO 27001	PRINCE2			
Mindestanforderungen	***Themen***	***Prinzipien***	***Techniken***	***Managementansätze***
Verwaltung der Werte	Änderungen			Änderungssteuerungsansatz
Zugangssteuerung		Definierte Rollen und Verantwortlichkeiten		Kommunikationsmanagementansatz
Kryptographie				Kommunikationsmanagementansatz
Physische und umgebungsbezogene Sicherheit				Kommunikationsmanagementansatz
Betriebssicherheit	Änderungen			Änderungssteuerungsansatz
Kommunikations-sicherheit		Definierte Rollen und Verantwortlichkeiten		Kommunikationsmanagementansatz
Anschaffung, Entwicklung und Instandhaltung von Systemen	Pläne, Qualität, Änderungen	Produktorientierung	Produktbasierte Planung, Qualitätsprüfungstechnik	Änderungssteuerungsansatz
Lieferantenbeziehungen	Organisation	Definierte Rollen und Verantwortlichkeiten		
Handhabung von Informations-sicherheitsvorfällen	Änderungen	Steuern nach dem Ausnahmeprinzip		
Business Continuity Management	Änderungen	Lernen aus Erfahrungen		Änderungssteuerungsansatz
Compliance	Business Case	Fortlaufende geschäftliche Rechtfertigung		Managementansätze für Qualität, Risiko und Kommunikation, Änderungssteuerungsansatz
Merkmale				
Angemessenheit		Anpassen an die Projektumgebung		

Tabelle 2: Gegenüberstellung der ISO 27001- und der PRINCE2-Bestandteile

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Business Case

Die ISO 27001 fordert ein, dass sich eine Organisation der Bedeutung von IS hinsichtlich der Erreichung der Organisationsziele bewusst ist und das ISMS angemessen und entlang der unternehmerischen Notwendigkeiten auf den Zweck und die Ziele des Unternehmens ausrichtet. Die Norm spricht hier vom "Kontext der Organisation" (DIN 2017, S. 6, Kap. 4.0).

Diese Anforderung gilt auch für Projekte. Im Rahmen der Erstellung des *Business Cases* muss deshalb begründet werden, in welchem Bezug das Projekt zur Trägerorganisation und zum Auftraggeber steht und wie das Projekt die Erreichung derer Ziele unterstützen kann. Welchen Nutzen hat das Unternehmen davon? Welcher Schaden kann hervorgerufen werden? Voraussetzung ist, dass Sie definiert haben, welche Bedeutung das Thema Informationssicherheit im Projekt hat.

Um den Anforderungen an Informationssicherheit gerecht zu werden, muss deshalb auch bestimmt werden:

- welche Bedeutung das Thema Informationssicherheit im Projekt hat
- welche Risiken oder Nutzeffekte sich für die Informationssicherheit aus der Durchführung des Projekts ergeben
- in wie weit Informationssicherheitsvorgaben eine signifikante Beschränkung für das Projekt darstellen
- ob sich zusätzliche Projektkosten oder Ressourcenbedarfe aus dem Betrieb eines ISMS im Projekt und der Einhaltung besonderer informationssichernder Anforderungen ergeben
- welche berechtigten Erwartungen interessierter Parteien bezüglich des Managements von Informationssicherheit bestehen
- wie der Anwendungsbereich von Maßnahmen zur Sicherung von Informationen im Projekt festgelegt und dokumentiert wird

Organisation

Das Thema Organisation umfasst definierte Rollen und Verantwortlichkeiten, die regeln, welche Rechte und Pflichten eine Rolle im Rahmen des Projektmanagements übernimmt. Hier gilt es die Anforderung der ISO 27001 hinsichtlich Führung und Unterstützung zu integrieren. Beispiele hierfür sind bereits beim Prinzip "Definierte Rollen und Verantwortlichkeiten" aufgeführt (s.o.).

Risiko

Eine Kernaufgabe des Projektmanagements ist das Risikomanagement, um Gefahren und Chancen für das Projekt zu erkennen und zu behandeln, damit die Erfolgswahrscheinlichkeit des Projektvorhabens steigt. Die ISO 27001 fordert ebenfalls ein Risikomanagement im Rahmen der Planung des ISMS. Dabei sollen Maßnahmen zum Umgang mit Risiken und Chancen identifiziert und Ziele für Informationssicherheit abgeleitet werden.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Beispiele zur Einbindung der Informationssicherheit in das Risikomanagement eines Projekts:

- Der *Risikomanagement-Ansatz (Risikomanagementstrategie)* berücksichtigt auch Risiken aus dem Bereich der Informationssicherheit und stellt (standardisierte) Maßnahmen bereit.
- Dokumentation im *Risikomanagement-Ansatz*
- Im *Risikoregister* gibt es eine eigene Kategorie "Informationssicherheit".
- Die Risikoeigentümer für IS-Risiken werden benannt. Die Rolle des IS-Verantwortlichen des Unternehmens im Projekt ist definiert.
- Das Risikobudget berücksichtigt Kosten für Maßnahmen zur Behandlung von IS-Risiken (Ersatz für Hardware-Schäden, Personalbudget für Betrieb des Projekt-ISMS usw.)

Pläne

Pläne und der zu Grunde liegende Planungsansatz geben den Projektbeteiligten Orientierung im Projekt und liefern die Referenz, um Planabweichungen zu messen. Die Projektplanung muss sowohl Ziele als auch Maßnahmen der Informationssicherheit berücksichtigen, da diese erhebliche Auswirkungen auf Kosten und Dauer des Projekts haben können. Um das betrieblich geforderte Sicherheitsniveau aufrecht zu erhalten, können z.B. zusätzlich IS-Maßnahmen im Projekt erforderlich sein oder für risikobehaftete Projektaktivitäten nur bestimmte Zeitfenster zur Verfügung stehen.

Beispiel: Sind Software-Rollouts aus Sicherheitsgründen nur in der Nacht und an Wochenenden möglich, so hat das Einfluss auf die Dauer des Projekts und auf die notwendigen Ressourcen (z.B. Mitarbeiterverfügbarkeit, Zulagen für Nacht- und Wochenendarbeit). Diese Effekte sind bei der Planung zu berücksichtigen. Der Auftraggeber ist über die Auswirkungen auf Kosten, Termine, Umfang, Qualität, Nutzen und Risiko zu informieren. Er kann darüber entscheiden, ob Sonderregelungen zugunsten der Projektplanung getroffen werden sollen, muss diese dann aber dokumentiert und unter Berücksichtigung aller bekannten Risiken begründen.

Änderungen

Änderungen an Baselines wie *Plänen* und *Produktbeschreibungen* können dazu führen, dass Projekte ihren ursprünglich geplanten Umfang verlieren, Toleranzen überschritten werden, Arbeitsergebnisse nicht wie eingefordert erstellt werden oder sich der erhoffte Nutzen für die Organisation nicht einstellt. Daher ist es notwendig, jeden *Änderungsantrag* auf seine Notwendigkeit und Auswirkungen (Zeit, Kosten, Qualität, Nutzen, Umfang und Risiko) zu prüfen, bevor der Änderung zugestimmt wird. Die Mindestanforderung für die Integration eines ISMS ist daher, bei der Risikobetrachtung von *offenen Punkten* immer auch die Auswirkungen auf den Betrieb informationsverarbeitender Einrichtungen und das ISMS selbst zu berücksichtigen.

Informationssicherheit betrachtet die Änderungssteuerung hinsichtlich der Auswirkungen auf den störungsfreien Betrieb von informationsverarbeitenden Einrichtungen und -prozessen. Denn Änderungen an Produkten können Folgen für die Aufrechterhaltung der IS haben oder Änderungen an der IS bedingen. Hinzu kommt das Management der Änderungen an schützenswerten Management- und Spezialisten-Produkten sowie Änderungen am ISMS selbst.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Beispiele für die Berücksichtigung von IS-Aspekten bei der Änderungssteuerung

- Änderungen bei der Bereitstellung von Dienstleistungen und Produkten durch Lieferanten werden gesteuert. Solche Änderungen umfassen auch die Pflege und Verbesserung bestehender Richtlinien, Verfahren und Maßnahmen der Informationssicherheit. Dabei werden die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet.
- Änderungen der Organisation, der Geschäftsprozesse, der informationsverarbeitenden Einrichtungen und der IT-Systeme werden gesteuert.
- Die Organisation beurteilt und überwacht Änderungen und ihre Folgen auf die Informationssicherheit. Sie ergreift ggf. korrigierende Maßnahmen, um das geforderte Niveau der Informationssicherheit zu gewährleisten.
- Die Lenkung dokumentierter Information umfasst auch die Überwachung von Änderungen (z.B. durch eine Versionskontrolle)
- Die Organisation beurteilt Risiken für die Informationssicherheit neu, wenn erhebliche Änderungen vorgeschlagen werden.
- Änderungen an sicherheitsrelevanten IT-Systemen innerhalb des Entwicklungszyklus werden durch formale Verfahren zur Verwaltung von Änderungen gesteuert.

Fortschritt

Die Fortschrittsmessung überwacht kontinuierlich die Umsetzung und die Durchführbarkeit der *Pläne*. Die Norm ISO 27001 fordert die Bewertung der Projektleistung (DIN 2017,A6.1.5) hinsichtlich der Informationssicherheitsleistung und der Wirkungsweise des ISMS (DIN 2017, Kap. 9). Das Ziel ist die fortlaufende Verbesserung der Informationssicherheitsleistung. Dies setzt voraus, dass dafür definiert wurde, welche Informationswerte und Schutzmaßnahmen im Projekt existieren und welche Methoden zur Leitungsmessung angewendet werden.

Für die Leistungsmessung empfiehlt die Norm regelmäßige interne Audits und Managementbewertungen. Auditoren finden Hinweise zur geforderten Informationssicherheitsleistung im *Kommunikationsmanagement-Ansatz (Kommunikationsmanagementstrategie)* und im *Business Case*. Im *Business Case* sind die Anforderungen an Informationssicherheit im Projekt und damit das angestrebte Schutzniveau zu definieren. Der *Kommunikationsmanagement-Ansatz* beschreibt, wer mit wem über welchen Kanal welche Information austauschen darf und muss, um dieses Schutzniveau zu ermöglichen. Diese Informationen dienen als Referenz für die Audits und Managementbewertungen.

Projektmanagement-Prozesse und Managementprodukte

Projektmanagementprozesse definieren die für das erfolgreiche Lenken, Managen und Liefern eines Projekts notwendigen Aktivitäten. Die Managementprodukte sind Eingangs- und Ausgangsgrößen dieser Prozesse.

Anforderungen an Informationssicherheit in Projekten werden von der Unternehmensleitung oder dafür bestimmten Rollen an die Projektsteuerung kommuniziert. Gelten diese Anforderungen für alle Arten von Projekten, können diese einmalig durch die Unternehmensleitung an die Verantwortlichen für das PMS kommuniziert werden, so dass diese die IS-Anforderungen im PMS integrieren.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Muss Ihr Projekt besonderen oder zusätzlichen Anforderungen an die Informationssicherheit genügen, werden diese mit dem *Projektmandat* von der Unternehmensleitung kommuniziert. Diese Anforderungen werden dann in den Projektzielen und dem *Lösungsansatz* berücksichtigt. Der Lenkungsausschuss überprüft dann im Prozess "Lenken eines Projekts" (s.u.) deren Einhaltung und evtl. bestehenden Anpassungsbedarf gemeinsam mit den anderen Projektzielen.

Der Grundstein für ein wirksames Projektmanagement wird z.B. bei PRINCE2 in den Prozessen "Vorbereiten eines Projekts" und "Initiieren eines Projekts" gelegt. Bereits hier ist es sinnvoll, Anforderungen zur Sicherheit von Informationen zu berücksichtigen, um eine effiziente Bearbeitung des Themas Informationssicherheit zu ermöglichen. Integrieren Sie Anforderungen an die Informationssicherheit deshalb von Projektbeginn an in diese Prozesse, deren Aktivitäten und Produkte. Stellen Sie dabei sicher, dass der Projektorganisation die Anforderungen an Informationssicherheit bekannt sind.

Prozess	Deutsche Übersetzung
Starting up a project	Vorbereiten eines Projekts
Directing a project	Lenken eines Projekts
Initiating a project	Initiieren eines Projekts
Controlling a stage	Steuern einer Phase
Managing product delivery	Managen der Produktlieferung
Managing a stage boundary	Managen eines Phasenübergangs
Closing a project	Abschließen eines Projekts

Tabelle 3: Die sieben Projektmanagement-Prozesse von PRINCE2

Vorbereiten eines Projekts

PRINCE2 definiert mit dem Prozess "Vorbereiten einer Projekts" Aktivitäten die vor dem Beginn des Projekts durchzuführen sind. Dies dient zum einen der bewussten Entscheidung, ob sich das Initiieren eines Projekts lohnt, zum anderen der Definition der Rahmenbedingungen für die Projektplanung. Dementsprechend sind bereits hier die Grundlagen für die Integration der Informationssicherheit in das Projekt zu definieren.

Aktivität: Am Anfang eines Projekts ernennen Sie das Projektmanagementteam; ggf. stellen Sie bereits das Projektteam zusammen. Achten Sie dabei auf eine angemessene Sicherheitsüberprüfung der Mitarbeiter. Die dafür geschlossenen Beschäftigungsverhältnisse und Verträge müssen die IS-Anforderungen berücksichtigen.

Aktivität: Gemäß des Prinzips "Lernen aus Erfahrung" erfassen Sie vorhandene Erfahrungen. Prüfen Sie dabei frühere Erfahrungen im Umgang mit Informationssicherheit in Projekten und berücksichtigen Sie diese für den *Lösungsansatz* und die weitere Planung.

Managementprodukte *Projektmandat* und *Business Case*: Informationssicherheit ist explizit Teil der Projektziele oder implizit (über das PMS) Teil der Bedingungen für die Genehmigung der Initiierung. Nur wenn auch die Einhaltung der ISMS-Ziele gewährleistet ist, kann die Initiierung des Projekts genehmigt werden. Alternativ müssen bewusste und dokumentierte Ausnahmeregelungen getroffen und Maßnahmen zur Steuerung vereinbart werden.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Managementprodukt *Projektbeschreibung*: Toleranzen für Informationssicherheit werden in Abstimmung mit dem Lenkungsausschuss vereinbart.

Managementprodukt *Lösungsansatz*: Das Vorgehen und die Mittel, um die Anforderungen an das ISMS zu erfüllen, werden benannt.

Lenken eines Projekts

Letztverantwortlich für die Informationssicherheit in einem Unternehmen ist stets die Geschäftsführung. So sieht es die ISO 27001 (DIN 2017, Kap. 5). Die Schnittstelle zur Unternehmensleitung und den Anforderungen des Business gewährleistet im Projektumfeld der Lenkungsausschuss. Der Lenkungsausschuss muss somit die Interessen der übergeordneten Organisation und Vorgaben zu Leit- und Richtlinien der Informationssicherheit an das Projekt weitergeben und deren Einhaltung überwachen. Änderungen im organisationseigenen ISMS werden dem Projektmanager zur Berücksichtigung mitgeteilt. Der Lenkungsausschuss kann diese z.B. an die Projektsicherung delegieren.

Aktivität: Der Lenkungsausschuss gibt Managementprodukte und Ressourcen frei unter Berücksichtigung der Anforderungen an die Informationssicherheit. Insbesondere betrifft dies die Freigabe des Projekts, der Managementphasen und des Projektendes. An Managementprodukten gibt er u.a. frei: *Lösungsansatz*, *Projektbeschreibung*, *Business Case*, *Phasenpläne*, *Projektleitdokumentation* sowie die *Management-Ansätze* für *Qualität, Risiko* und *Kommunikation* sowie den *Änderungssteuerungsansatz*.

Umgekehrt stellt der Projektmanager sicher, dass Berichte an den Lenkungsausschuss, wie *Ausnahme-*, *Projektstatus-* und *Phasenabschlussberichte* auch über den Status der Informationssicherheit berichten, sofern dies auf Managementebene relevant, bzw. mit dem Lenkungsausschuss vereinbart ist. Vereinbarungen hierzu werden im *Kommunikationsmanagement-Ansatz* dokumentiert.

Wenn der Projektmanager Probleme mit Lieferanten und Lieferantenverträgen im Hinblick an Anforderungen zur Informationssicherheit nicht klären kann, vermittelt der Lenkungsausschuss in der Rolle des Lieferantenvertreters.

Initiieren eines Projekts

Dieser Prozess liefert mit der *Projektleitdokumentation* die Entscheidungsgrundlage für den Lenkungsausschuss, das Projekt zu genehmigen oder abzulehnen. Zu diesem Zweck wird eine Reihe von grundlegenden Managementprodukten aktualisiert bzw. erstellt, wie unter anderem der *Business Case* und der *Projektplan*. Deshalb sollte im Prozess "Initiieren eines Projekts" auch definiert werden, wie im Projekt konkret das ISMS zu integrieren ist, z.B. wie mit Risiken und *offenen Punkten* (inkl. *Änderungsanträgen*) bzgl. Informationssicherheit umzugehen ist.

Hierzu muss als erstes das Niveau der Informationssicherheit bestimmt werden. Drei Leitfragen helfen dabei, die richtige Skalierung für das ISMS im Projekt zu finden:

1. Was muss gemacht werden?
2. Worauf kann verzichtet werden?
3. Was kann in kleiner Ausprägung, was muss in erweitertem Umfang betrieben werden?

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Jegliche Abweichung von Standardvorgehen der Trägerorganisation muss mit dem Lenkungsausschuss und der Projektsicherung abgestimmt und dokumentiert werden.

Managementprodukt *Risikomanagement-Ansatz (Risikomanagementstrategie)*: Dieses Managementprodukt berücksichtigt ISMS-Aspekte hinsichtlich Identifikation und Umgang im IS-Risiken, IS-Toleranzen, zuständigen Rollen und zu verwendenden Werkzeugen und Techniken zur Steuerung der IS-Risiken. Das *Risikoregister* enthält erste identifizierte Informationssicherheitsrisiken.

Managementprodukt *Kommunikationsmanagement-Ansatz (Kommunikationsmanagementstrategie)*: Dieses Managementprodukt definiert, wer Projektinformationen berechtigt einsehen und ändern darf, welche Werkzeuge und Verfahren zur Übermittlung und dem Abruf von Informationen verwendet werden dürfen. Sie eignet sich daher auch gut, um wesentliche Rahmenbedingungen für den Umgang mit Informationen im Projekt zu definieren. Personen oder Rollen werden hier hinsichtlich ihrer Verantwortungsbereiche benannt und über ihre Rechte und Pflichten aufgeklärt. Werkzeuge und Verfahren zur Sicherstellung der Wahrung von Informationssicherheit bei der Übertragung werden vereinbart.

Beispiele für die Berücksichtigung der Informationssicherheit im Kommunikationsmanagement-Ansatz

- Regeln für den Umgang mit Aufzeichnungen, Berichten und Mitarbeiterdaten (z.B. Vervielfältigung, Entsorgung und Transport von Datenträgern)
- Richtlinien zum Einsatz von Mobilgeräten, zur Installation von Software, zur privaten Benutzung von dienstlicher IT, zum Einsatz von Verschlüsselung und zur Heimarbeit
- Steuerung von Zugangsrechten durch einheitliche technische Rollen- und Rechtekonzepte für Projektrollen
- Definition von Schutzstufen für Informationen und deren Datenträger
- Anforderungen für projekteigene Laufwerke oder Netzwerkdomänen
- Vereinbarungen zur Vertraulichkeit oder Geheimhaltung (Haftung im Schadenfall)
- Vereinbarungen zur Informationsübertragung (Rollen, Verantwortungen, Haftung), z.B. elektronische Signaturen und Verschlüsselung bei elektronischen Nachrichten
- Richtlinien zum Löschen, Erhalt und Archivieren von Informationen nach Projektende

Managementprodukt *Qualitätsmanagement-Ansatz (Qualitätsmanagementstrategie)*: Dieses Managementprodukt definiert das im Projekt anzuwendende Qualitätsmanagementsystem. Damit ist es der geeignete Ort, um das geforderte Niveau an Informationssicherheit festzulegen und diesbezüglich zu berücksichtigende ISMS-Aspekte und Organisationsstandards aufzuführen.

Beispiele für die Berücksichtigung der Informationssicherheit im Qualitätsmanagement-Ansatz:

- Definition des einzuhaltenden Qualitätsniveaus für Informationssicherheit
- Vereinbarungen zu Qualitätstoleranzen für die Informationssicherheit

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

- Anforderungen an Lieferanten hinsichtlich Informationssicherheit, erwarteter Qualitätslevel (z.B. ISO 27001-Zertifizierung, datenschutzkonformes Arbeiten etc.)
- Benennung geeigneter Prüfverfahren für die Qualität der Informationssicherheit
- Vereinbarungen zu Rollen & Verantwortlichkeiten für die Qualität der Informationssicherheit
- Benennung geeigneter Verfahren zur Auditierung des ISMS im Projekt
- Vereinbarungen hinsichtlich zu verwendender Werkzeuge und Techniken zum Management der Qualität von Informationssicherheit

Managementprodukt *Änderungssteuerungs-Ansatz (Konfigurationsmanagementstrategie)*: In diesem Managementprodukt wird das Änderungssteuerungsverfahren definiert. PRINCE2 setzt ab der Version 2017 voraus, dass die Projektumgebung das Konfigurationsmanagement zur Verfügung stellt (Verwaltung der Produkte wie z.B. Ablageorte und Konfigurationsdatensätze). Sowohl Management- als auch Spezialistenprodukte sind die im Projekt entstehenden Informationswerte. Die ISO 27001 fordert, Informationen so zu lenken, dass sie verfügbar und angemessen geschützt sind. Deshalb ist es unverzichtbar, die Aspekte der Informationssicherheit für den Umgang mit Konfigurationselementen zu definieren.

So sollte festgelegt werden, wie und von wem Produkte und deren Informationswerte bearbeitet und geschützt werden. Zusätzlich sollten auch explizite ISMS-Aspekte in Bezug auf Management- und Spezialisten-Produkte bei der Ausarbeitung des *Änderungssteuerungs-Ansatzes* berücksichtigt werden. Z.B. hinsichtlich der Anforderungen aus dem organisationseigenem ISMS an Konfigurationsmanagementsysteme. Dies erfolgt unter Berücksichtigung identifizierter ISMS-Risiken (aus dem *Risikoregister* und *Projekttagebuch* und möglicher Erfahrungen aus früheren Projekten).

Beispiele für die Berücksichtigung der Informationssicherheit im Änderungssteuerungs-Ansatz:

- Inventarisierung der Informationswerte (Für welche Informationswerte ist die Projektorganisation verantwortlich? Welche Schutzstufe besteht?)
- Verantwortlichkeit für die Sicherheit der Informationswerte (pro Applikation, Standort etc.)
- Klassifizierung, Kennzeichnungspflichten und Verfahren für Informationen und deren Datenträger hinsichtlich Schutzstufen (low, medium, high, critical)
- Existieren auf Organisationsebene bereits Vorgaben zur Versionierung von Dokumenten? Können diese für Projektinformationen übernommen werden?
- Gibt es Vorgaben zur Projektablagestruktur?
- Regelungen für die Handhabung von Speicher- und Aufzeichnungsmedien
- Verfahren und Verantwortlichkeiten zur Behandlung *offener Punkte* (*Änderungsanträge)*

Aktivität: Die umfangreichste Aufgabe bei der Initiierung eines Projekts ist es, den *Projektplan* zu erstellen. Im Projektmanagement dienen Pläne der Orientierung im Projekt und der Messung von Planabweichungen. Aus Sicht der Informationssicherheit müssen bei der Projektplanung auch die Ziele für Informationssicherheit und die

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

dazugehörigen Maßnahmen eines Projekts berücksichtigt werden. So kann die Berücksichtigung betrieblicher Anforderungen zur Aufrechterhaltung des Informationssicherheitsniveaus Auswirkungen auf Dauer oder Zeitpunkte von Projektaktivitäten haben. Bei der Kalkulation der Kosten sind ggf. Kosten für IS-Maßnahmen im Planbudget zu berücksichtigen. Das Thema Pläne (s.o.) definiert die Anforderungen an die Projektplanung.

Managementprodukt *Business Case*: Mit den Daten der detaillierten Projektplanung arbeitet der Projektmanager den endgültigen *Business Case* aus. Dieser dient dem Lenkungsausschuss als zentrale Entscheidungsgrundlage für Genehmigung oder Ablehnung des Projekts. Der ausgearbeitete *Business Case* dokumentiert die Gründe für die Durchführung eines Projekts, spezifiziert den erwarteten Nutzen und gibt einen Überblick über daraus resultierende Risiken. Das Thema Business Case (s.o.) beschreibt die Qualitätskriterien für das Managementprodukt *Business Case*.

Aktivitäten: Der Prozess "Initiieren eines Projekts" endet mit dem Einrichten der Projektsteuerungsmittel und dem Zusammenstellen der *Projektleitdokumentation* (diese enthält u.a. den *Business Case*) als Entscheidungsvorlage für den Lenkungsausschuss. Dabei prüft das Projektmanagementteam die Managementprodukte noch einmal auf Ihre Wirkungsweise, Angemessenheit und Konsistenz. Beteiligte Rollen müssen der Übernahme ihrer Aufgaben im Sinne der definierten Managementansätze zustimmen.

Folgende Rollen können geeignet sein, um an diesen Aktivitäten mitzuwirken:

Die Projektunterstützung:

- Review der Dokumente auf Konformität mit den Anforderungen aus dem PMS. Wurden erste Aussagen zu IS-Anforderungen berücksichtigt?
- Zusage, die administrative Abwicklung von Qualitätsprüfungsprozessen zu unterstützen,
- das Änderungssteuerungsverfahren verwalten.
- Zusage, Berichte zu IS-Vorfällen zusammenzustellen sowie die abgesprochenen Tools und Techniken zu betreiben.

Die Projektsicherung:

Review der erstellten Dokumente hinsichtlich IS-Anforderungen zu Änderungssteuerung, Kommunikations-, Qualitäts- und Risikomanagement im Sinne des Unternehmens, der Benutzer und der Lieferanten

Die Qualitätssicherung:

Diese ist eine Rolle der Trägerorganisation (unabhängig vom Projekt). Sie sollte über Spezialistenkenntnisse zur Informationssicherheit und verwandten Standards verfügen und damit die Projektsicherung unterstützen. Die Qualitätssicherung beurteilt, ob die gewählten Steuerungsmittel hinsichtlich Informationssicherheit angemessen sind.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Der Lenkungsausschuss

Dieser prüft anschließend im Prozess "Lenken eines Projekts" (s.o.) die *Projektleitdokumentation*. Er entscheidet über den *Projektplan* inklusive der abgestimmten Phasen und Toleranzen, den *Business Case*, die vorgeschlagenen Steuerungsmittel, den *Lösungsansatz* und die vorgeschlagene Zusammensetzung des Projektteams. Dabei berücksichtigt er – z.B. bei der Vergabe von Aufträgen an Dienstleister – die Anforderungen an Informationssicherheit.

Steuern einer Phase

Das Steuern einer Phase entspricht der täglichen Arbeit eines Projektmanagers.

Aktivitäten: Erfassen und Prüfen *offener Punkte* zum Thema Informationssicherheit, Identifizieren und Überwachen von Risiken für die Informationssicherheit im *Risikoregister*, Aufnahme von Qualitätsaktivitäten für die Informationssicherheit im *Qualitätsregister*.

Aktivität: Droht das Niveau für Informationssicherheit aus den Toleranzen zu geraten, plant der Projektmanager geeignete Korrekturmaßnahmen, delegiert sie und überprüft ihre Wirksamkeit gemäß des PDCA-Zyklus.

Aktivitäten: Bei der Freigabe von *Arbeitspaketen* sind ggf. Anforderungen an Informationssicherheit mit dem Teammanager zu vereinbaren (Beispiel: Software muss Daten nach einem zu bestimmenden Sicherheitsniveau verschlüsseln können). Das Prüfen des Arbeitspaketstatus umfasst auch die Informationssicherheit. Wenn der Projektmanager das abgeschlossene *Arbeitspaket* entgegennimmt, muss er prüfen, ob die Anforderungen an die Informationssicherheit erfüllt wurden.

Aktivitäten: Der Projektmanager berücksichtigt beim Prüfen des Phasenstatus und beim Erstellen von *Projektstatusberichten* auch Aspekte der Informationssicherheit.

Managen der Produktlieferung

Lieferantenverträge berücksichtigen grundlegende IS-Anforderungen in Bezug auf die zu liefernden Dienstleistungen. *Arbeitspakete* enthalten detaillierte Aussagen zu Anforderungen an Informationssicherheit und bei der Auswahl von Dienstleistern wird deren Eignung zum Umgang mit unternehmenskritischen Informationen geprüft (z.B. durch eine ISO 27001-Zertifizierung). Im Rahmen der Übergabe von *Arbeitspaketen* werden die gelieferten Produkte auch hinsichtlich der vorher gesetzten Anforderungen an Informationssicherheit geprüft und abgenommen.

Managen eines Phasenübergangs

In diesem Prozess prüft der Projektmanager, ob das Projekt noch in der Lage ist, innerhalb der gesetzten Vorgaben den *Business Case* zu erfüllen. Dies umfasst auch die Anforderungen des Informationssicherheitsmanagements, die im *Business Case* enthalten sind. Daraus leitet er eine Entscheidungsvorlage für den Lenkungsausschuss ab, in der er entweder den vorzeitigen Projektabschluss empfiehlt oder die nächste Phase beantragt.

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

Das Managen eines Phasenübergangs enthält folgende Aktivitäten:

Über Phasenabschluss berichten: Spätestens zum Ende einer Phase wird gemessen, in welchem Maß die IS-Anforderungen erreicht wurden. Abweichungen und deren Gründe werden im *Phasenabschlussbericht* erfasst und ihre Auswirkungen auf das Projekt kommuniziert.

Pläne prüfen und anpassen: Sind Informationssicherheitsvorfälle, Schwierigkeiten mit den gewählten Informationssicherungsverfahren oder Anpassungen hinsichtlich Informationssicherheit Anlass für Planabweichungen, führen diese zu Aktualisierungen am *Projektplan*. Dieser bedarf der Abnahme durch den Lenkungsausschuss.

Business Case aktualisieren: Können für die Ausführung des Projekts wichtige Anforderungen an Informationssicherheit nicht oder nicht innerhalb der Vorgaben erfüllt werden, muss am Phasenende überprüft werden, ob der *Business Case* unter diesen Bedingungen noch zu erfüllen ist. Das Ergebnis kann die Aktualisierung des *Business Cases* oder Überlegungen zum Abschließen des Projekts sein.

Projektsteuerungsmittel anpassen: Ergibt sich, dass die gewählten Steuerungsmittel nicht geeignet sind, um die Projektziele zu erreichen, können diese für die nächste Phase angepasst werden.

Nächste Phase planen: Im Plan für die nächste Phase (ggf. als *Ausnahmeplan*) werden Erkenntnisse und Vorgaben zum Umgang mit Informationssicherheit im Projekt berücksichtigt. Diese können Auswirkungen auf den Projektverlauf (Zeit, Kosten, Qualität) haben.

Abschließen eines Projekts

Naht das Ende eines Projekts, wird der Projektabschluss unter Berücksichtigung der Anforderungen aus der Informationssicherheit gesteuert. Geplant werden diese Tätigkeiten bereits gegen Ende der vorherigen Managementphase im Prozess "Managen eines Phasenübergangs".

Spezialistenprodukte: Berücksichtigen Sie bei den Abnahmen des Projekts und der Spezialistenprodukte auch IS-Anforderungen. Überprüfen Sie, ob das *Projektendprodukt* die dokumentierten Anforderungen an den Umgang mit Informationssicherheit gewährleistet und geeignet ist, den zukünftig erwarteten Nutzen zu erfüllen.

Managementprodukt *Projektabschlussbericht*: Der *Projektabschlussbericht* kann benutzt werden, um zu berichten, in wie weit zuvor gesetzte Anforderungen an die Informationssicherheit im Projektmanagement und in Bezug auf die zu erstellenden Produkte erfüllt werden konnten. *Offene Punkte* und Erkenntnisse zu Nachbesserungsarbeiten hinsichtlich IS-Anforderungen müssen hier gelistet werden. Auch Einschätzungen zum Reifegrad der Projektorganisation hinsichtlich der Fähigkeit zur Umsetzung von IS-Anforderungen können hier hilfreich sein.

Managementprodukt *Erfahrungsbericht*: Basierend auf den Einträgen zur Kategorie "IS" aus dem *Erfahrungsprotokoll* wird ein *Erfahrungsbericht* erstellt, in dem z.B. Lösungen zum Umgang mit Informationssicherheitsrisiken oder Empfehlungen zu Nachbesserungsarbeiten an IS-Richtlinien kommuniziert werden. Dies gilt insbesondere, wenn sie für die weiterführende Verwendung in anderen Projekten geeignet sind. Der *Erfahrungsbericht* sollte auf jeden Fall an das für

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion

das Qualitätsmanagement zuständige Büro von Trägerorganisation und Auftraggeber weitergegeben werden, damit notwendige Änderungen an Richtlinien und Standards vorgenommen werden können.

Managementprodukt *Empfehlungen für Folgeaktionen*: Es ist sicherzustellen, dass nach Projektende die Projektinformationen gemäß den Vorgaben des ISMS archiviert, sicher gelöscht oder an die zuständige Stelle übergeben wird.

Betriebsmittel: Geeignete Verfahren sollten implementiert sein, um sicherzustellen, dass Mitarbeiter und Lieferanten für das Projekt bereitgestellte Informationswerte zurückgeben oder diese ihnen entzogen werden (z.B. Ausweise mit erweiterten Zutrittsberechtigungen, Accounts, Laptops, Akten).

Projektumfeld

Sowohl PRINCE2 als auch die ISO 27001 empfehlen, die von ihnen bereitgestellten Managementmittel angemessen einzusetzen. Die unsachgemäße Anwendung beziehungsweise unangemessene Anpassung der Mittel führt sonst schnell zu einem merkbaren administrativen Mehraufwand ohne ausreichenden Nutzen. Anpassen bedeutet für beide Richtlinien: Nicht Weglassen, sondern Skalieren! So kann es z.B. bei einem kleinen Projekt vollständig ausreichend sein, die Projektablage im Rahmen der üblichen Datensicherung des Unternehmens zu sichern. Für ein Großprojekt mit mehreren beteiligten Unternehmen kann es hingegen erforderlich sein, eine mehrfache Datensicherung auf physikalisch getrennten Systemen vorzunehmen.

Empfehlungen für das Anpassen des ISMS an das Projektumfeld:

- Definieren Sie ISMS-Anforderungen in Abhängigkeit von Größe und Art des Projekts im Projektmanagement-Handbuch. Dann kann die explizite Benennung in *Projektmandat* und *Business Case* entfallen.
- Arbeiten Sie mit integrierten Managementsystemen, um den Mehraufwand für den Betrieb von zwei Systemen zu vermeiden.
- Berücksichtigen Sie das Prinzip der Angemessenheit bei den Maßnahmen zur Risikobehandlung.
- Schlagen Sie Gemeinkosten für den Betrieb von ISMS auf alle Projekte um.

Literatur

- AXELOS (Hrsg.): Managing Successful Projects with PRINCE2, 6th ed., UK, The Stationery Office Ltd TSO, 2017
- 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

© 2018 Projekt Magazin. Vervielfältigung, auch auszugsweise, nur mit schriftl. Genehmigung der Redaktion