thinkproject!

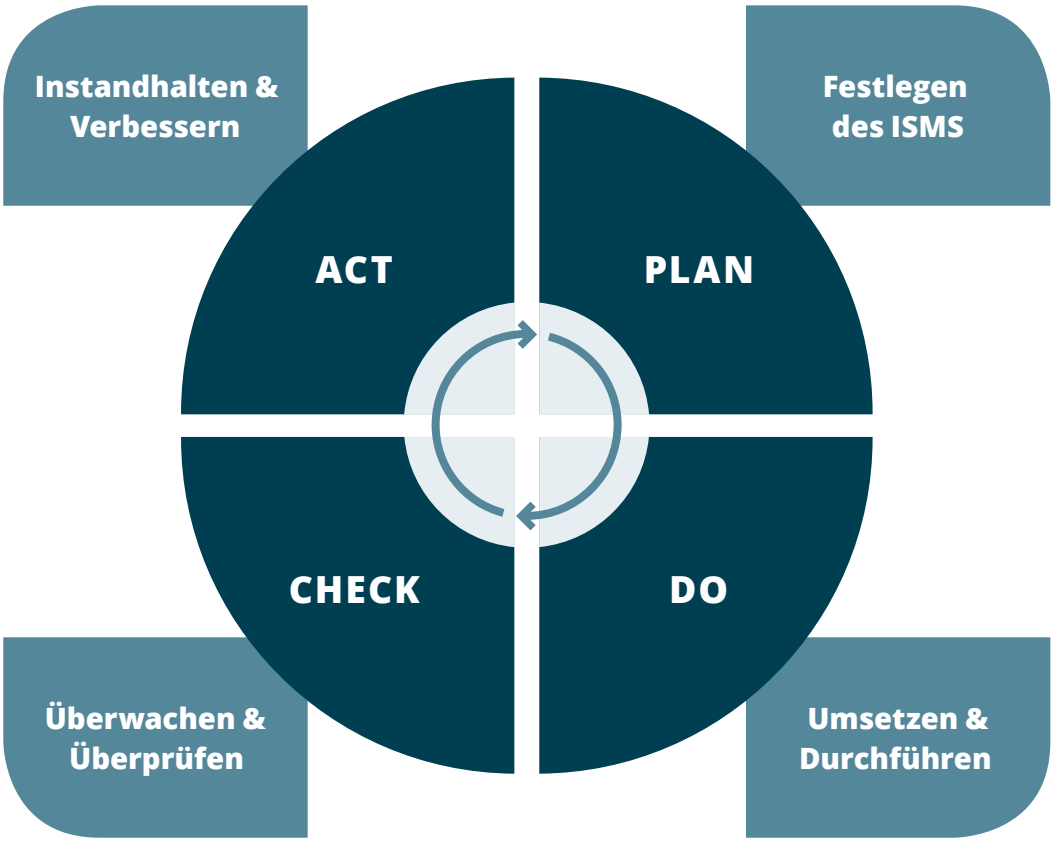
LEITLINIE INFORMATIONSSICHERHEIT

think project! Informationssicherheits-Managementsystem (ISMS)

Version 2.7 // 01.12.2016

thinkproject!

INFORMATIONSSICHERHEITSPROZESS (PDCA)



Dieses Dokument ist nur in der online verfügbaren Fassung gültig. Ausgedruckte und sonstige gespeicherte Fassungen unterliegen nicht dem Änderungsdienst.

Einstufung: Restricted

thinkproject!

INHALTSVERZEICHNIS

1 ÜBERBLICK UND VERBINDLICHKEITSERKLÄRUNG

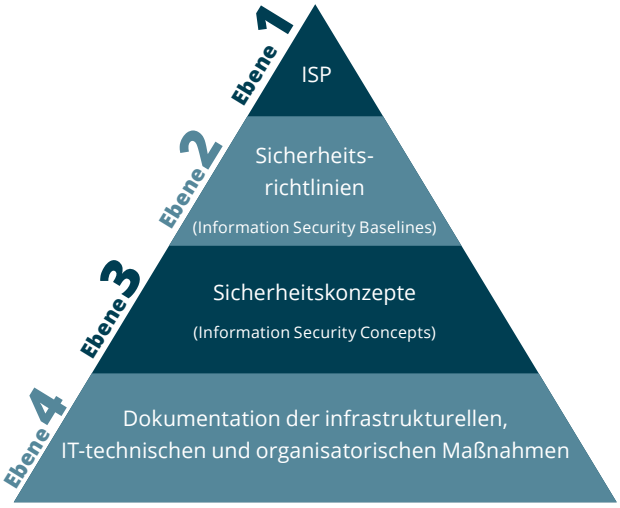
1.1 STELLENWERT DER INFORMATIONSSICHERHEIT

Für die think project! Unternehmen sowie für ihre Kunden hat die Informationssicherheit einen sehr hohen Stellenwert. Dies ist begründet durch eine hohe Abhängigkeit von einer effizienten und verfügbaren Informationsverarbeitung sowie durch die Anforderungen, die sich im Zusammenhang mit Corporate Governance, Risk Management und den Gesetzen zum Datenschutz ergeben. Die Informationssicherheit ist daher integraler Bestandteil der Unternehmensstrategie von think project!.

Die think project! Unternehmen, ihre Mitarbeiter und externen Dienstleister sind in hohem Maße verpflichtet, die Risiken der Informationsverarbeitung wie z. B. Datenabfluss, Datenmanipulation, technische Störungen oder Sabotage beherrschbar zu halten und auf ein vertretbares Maß zu reduzieren. Um diese Verpflichtung zu erfüllen, wurde ein Informationssicherheits-Managementsystem (ISMS) implementiert, das unternehmensweit geregelt und zentral koordiniert wird. Das vorliegende Dokument – die Information Security Policy – soll als übergeordnete Leitlinie sicherstellen, dass für den jeweiligen Schutzzweck angemessene und wirksame Sicherheitsmaßnahmen ergriffen werden.

1.2 ISMS DOKUMENTENSTRUKTUR

Die Information Security Policy (ISP) bildet die oberste Ebene der Dokumentation des ISMS.



Dokumentenstruktur eines ISMS

Jeder Mitarbeiter der think project! Unternehmen hat sich an die Information Security Policy und an die daraus abgeleiteten Standards und Richtlinien zu halten. Diese sollen Informationen der Kunden und der think project! Unternehmen schützen sowie deren Verfügbarkeit gewährleisten.

1.3 FREIGABE

Die Geschäftsleitung hat die vorliegende Information Security Policy nach Prüfung freigegeben. Alle Mitarbeiter sind angewiesen, diese Regelungen anzuwenden und durch verantwortungsvolles Handeln den Informationsschutz gesetzeskonform und wirkungsvoll zu leben.

1.4 KONTROLLE UND SANKTIONEN

Die Information Security Policy ist für jeden, der für oder mit den think project! Unternehmen im Rahmen des Anwendungsbereichs arbeitet (Mitarbeiter, Berater, Dienstleister, Lieferanten), verpflichtend. Die Einhaltung des ISMS wird regelmäßig und fallbezogen überprüft.

Jeder Mitarbeiter der think project! Unternehmen beachtet die Information Security Policy und die daraus abgeleiteten Standards und Richtlinien. Verstöße gegen die Anweisungen werden verfolgt und geahndet.

1.5 ANSPRECHPARTNER

Anfragen, Anregungen und Kritik sind jederzeit willkommen. Richten Sie diese, aber auch etwaige Beschwerden, bitte an den think project! Informationssicherheitsbeauftragten.

München, im Dezember 2016

Thomas Bachmaier
Geschäftsführer

2 DEFINITIONEN

2.1 INFORMATIONSSICHERHEIT

Informationssicherheit umfasst die Eigenschaften von informationsverarbeitenden Systemen und Organisationseinheiten, welche die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren und Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken.

2.2 ISMS

Unter einem Informationssicherheits-Managementsystem (ISMS) wird der Teil des unternehmensweiten Managementsystems verstanden, der auf Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit abdeckt. Das ISMS umfasst die Strukturen, Richtlinien, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen des Unternehmens.

2.3 INFORMATIONSEIGENTÜMER

Zu jedem informationsverarbeitenden Geschäftsprozess und jeder Fachanwendung ist ein Ansprechpartner benannt, der als Prozessverantwortlicher oder Informationseigentümer für alle Fragen der Informationsverarbeitung und der Informationssicherheit im Rahmen dieses Geschäftsprozesses verantwortlich ist. Die Verantwortlichen stellen sicher, dass die für diesen Geschäftsprozess relevanten Sicherheitsmaßnahmen dem Schutzbedarf entsprechen.

3 ZIELE UND GRUNDSÄTZE DER INFORMATIONSSICHERHEIT

3.1 ZIELE

Die Informationssicherheitsziele der think project! Unternehmen sind:

- Erfüllung der Kundenforderungen an Vertraulichkeit, Integrität und Verfügbarkeit
- Zuverlässige Unterstützung der Geschäftsprozesse durch die Informationstechnologien und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation
- Realisierung sicherer und vertrauenswürdiger Kommunikation mit Kunden, Behörden und externen Dienstleistern
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte
- Sicherung der hohen Werte der Informationen
- Erfüllung der aus gesetzlichen Vorgaben resultierenden Anforderungen
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der Verarbeitung personenbezogener Daten (Datenschutz)
- Reduzierung der im Schadensfall entstehenden Kosten

3.2 GRUNDSÄTZE

Bei der Erstellung von Informationssicherheitsrichtlinien und -konzepten sind folgende Grundsätze berücksichtigt:

3.2.1 Angemessenheit

Ziele von Sicherheitsmaßnahmen und der benötigte Aufwand stehen in einem angemessenen Verhältnis zueinander. Neben der Beachtung gesetzlich vorgeschriebener Sicherheitsanforderungen werden Sicherheitsmaßnahmen auch immer im Verhältnis zum Schutzzweck einer Angemessenheitsprüfung unterzogen.

3.2.2 Ressourcen

Zur Erreichung und Aufrechterhaltung eines angemessenen Maßes an Sicherheit sind ausreichende finanzielle, personelle und zeitliche Ressourcen bereitgestellt.

3.2.3 Einbindung der Mitarbeiter

Informationssicherheit betrifft jeden Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und sicherheitsbewusstes Handeln helfen, Schäden zu vermeiden.

3.2.4 Informationsklassifizierung

Alle Informationen, die im Rahmen von Geschäftsprozessen verarbeitet werden, sind anhand ihres Schutzbedarfs klassifiziert. Dies ist Voraussetzung für die Risikoanalyse und die Implementierung angemessener Schutzmaßnahmen.

4 VERANTWORTLICHKEITEN

4.1 EIGENVERANTWORTUNG

Jeder Mitarbeiter ist im Rahmen seiner Aufgabenerfüllung für die ihm anvertrauten Informationen und Prozesse bzw. Arbeitsschritte verantwortlich. Um dies zu unterstützen, ist die unternehmensinterne Sicherheitsorganisation klar strukturiert.

4.2 INFORMATIONSEIGENTÜMER

Der Informationseigentümer:

- stellt die geschäftliche Relevanz seiner Informationen und den Schutzbedarf fest.
- sorgt dafür, dass Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz seiner Informationen implementiert werden.

Der Informationseigentümer definiert die Zugriffsmöglichkeiten auf Informationen sowie die Art und den Umfang der Autorisierung, die im jeweiligen Zugriffsverfahren erforderlich sind. Dabei werden Aufbewahrungsvorschriften und die mit den Informationen verbundenen rechtlichen Anforderungen berücksichtigt.

4.3 PROZESSVERANTWORTLICHER

Der Prozessverantwortliche ist verantwortlich für das Definieren der prozessstrategischen Ziele und das Bereitstellen aller erforderlichen Ressourcen sowie die Durchführung unter Einhaltung der Gesetze und Vorschriften.

4.4 GESCHÄFTSLEITUNG

Die Geschäftsleitung stellt die personellen, organisatorischen und finanziellen Mittel bereit, um das ISMS im Unternehmen wirkungsvoll zu betreiben und zu verbessern. Bei ihr liegt ebenfalls die Verantwortung für die Bewertung der erreichten Standards der Informationssicherheit in Hinblick auf Wirksamkeit und Angemessenheit.

4.5 INFORMATIONSSICHERHEITSBEAUFTRAGTER

Der Informationssicherheitsbeauftragte (ISB) ist der Geschäftsleitung direkt als Stabsstelle zugeordnet. Er ist für die Aufrechterhaltung des ISMS zuständig und dafür verantwortlich, dass der Prozess der Informationssicherheit im Unternehmen gelebt wird. Er berät die Funktionsbereiche und berichtet regelmäßig sowie bei Bedarf ad hoc an die Geschäftsleitung über die Leistung der Sicherheitsmaßnahmen und über etwaige Sicherheitsvorfälle.

4.6 DATENSCHUTZBEAUFTRAGTER

Der Datenschutzbeauftragte wirkt auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hin. Er überwacht die datenschutzgerechte Anwendung der Datenverarbeitungsprozesse und berät die Funktionsbereiche in Fragen zum Datenschutz.

4.7 EINKAUF

Der Einkauf von IT-Komponenten und Dienstleistungen wird vom Funktionsbereich Systems Engineering durchgeführt und koordiniert. Soweit erforderlich sind die IT-Lieferanten und externen Dienstleister vertraglich auf die Einhaltung des Bundesdatenschutzgesetzes und anderer sicherheitsrelevanter Vorschriften verpflichtet.

4.8 CONTROLLING

Das Controlling legt ein besonderes Augenmerk auf die Kosten-Nutzen-Analyse von sicherheitsrelevanten Projekten und deren Betriebskosten.

5 SICHERHEITSOBJEKTE UND SCHUTZSTUFEN

Ausgehend von den zu schützenden Informationen ist der Schutzbedarf festgestellt. Der Schutzbedarf vererbt sich auf die Prozesse, IT-Anwendungen, Datenbanken, Server, Personal Computer, Netze, Räume usw. und gegebenenfalls auch auf Gebäude und Flächen.

Der Schutzbedarf wird konkretisiert durch die Schutzkategorien:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Verbindlichkeit

In jeder Schutzkategorie sind differenzierende Schutzstufen festgelegt.

5.1 VERTRAULICHKEIT

Vertraulichkeit ist die Eigenschaft einer Information, nur für einen beschränkten Empfängerkreis (Personen, Einheiten, Prozesse) vorgesehen zu sein.

Die Information ist vor unberechtigter Einsichtnahme geschützt und nicht ohne Erlaubnis des Eigentümers offenzulegen.

Schutzstufe	Beschreibungen
Open	Es ist keine Vertraulichkeit gegeben.
Restricted	Eine Verletzung der Vertraulichkeit wird als normales Risiko bewertet, wenn keine bis geringfügige Auswirkungen zu erwarten sind.
Confidential	Eine Verletzung der Vertraulichkeit wird als schwerwiegendes Risiko eingestuft, wenn spürbare Auswirkungen die Folge sein könnten. Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
Sensitive	Eine Verletzung der Vertraulichkeit wird als äußerst gravierendes Risiko bewertet, wenn sie den gesellschaftlichen und/oder wirtschaftlichen Ruin bedeuten könnte. Eine Beeinträchtigung der persönlichen Unversehrtheit ist möglich und es könnte eine Gefahr für Leib und Leben bestehen.

5.2 INTEGRITÄT

Integrität bezeichnet die Korrektheit (Unversehrtheit) und Vollständigkeit von Informationen und die korrekte Funktionsweise von Systemen. Die Informationen sind vor Verfälschung und Verlust zu schützen.

Schutzstufe	Beschreibungen
Normal	Ein Verlust der Integrität wird als normales Risiko bewertet, wenn keine bis geringfügige Auswirkungen zu erwarten sind.
Enhanced	Ein Verlust der Integrität wird als schwerwiegendes Risiko eingestuft, wenn spürbare Auswirkungen die Folge sein könnten. Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
High	Ein Verlust der Integrität wird als äußerst gravierendes Risiko bewertet, wenn er den gesellschaftlichen und/oder wirtschaftlichen Ruin bedeuten könnte. Eine Beeinträchtigung der persönlichen Unversehrtheit ist möglich und es könnte eine Gefahr für Leib und Leben bestehen.

5.3 VERFÜGBARKEIT

Verfügbarkeit ist ein Maß für den zeitlichen Umfang, in dem eine Information (ein System) für Geschäftsprozesse zur Verfügung steht. Diese Schutzkategorie ist als tolerierbare Ausfallzeit pro festgelegten Zeitrahmen definiert.

Schutzstufe	Beschreibungen
Normal	Ein Ausfall von Systemen oder Verlust der Verfügbarkeit von Informationen wird als normales Risiko eingeschätzt, wenn keine bis geringfügige Auswirkungen zu erwarten sind.
Enhanced	Ein Ausfall von Systemen oder Verlust der Verfügbarkeit von Informationen wird als schwerwiegendes Risiko eingeschätzt, wenn erhebliche Auswirkungen zu erwarten sind oder das öffentliche Ansehen oder Kundenbeziehungen geschädigt werden könnten.
High	Ein Ausfall von Systemen oder Verlust der Verfügbarkeit von Informationen wird als äußert gravierendes Risiko eingeschätzt, wenn sie den gesellschaftlichen und/oder wirtschaftlichen Ruin bedeuten würden oder das öffentliche Ansehen nachhaltig schädigen oder entscheidende Kundenbeziehungen dauerhaft beenden könnten.

Soweit in Einzelfällen erforderlich, werden als Schutzkategorien außerdem hinzugezogen:

5.4 AUTHENTIZITÄT

Authentizität ist die Eigenschaft der zweifelsfreien Zuordnung einer Nachricht oder Transaktion auf Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit zu einem eindeutigen Sender und/oder Empfänger.

5.5 VERBINDLICHKEIT

Verbindlichkeit (Nichtabstreitbarkeit) bedeutet, dass kein unzulässiges Abstreiten durchgeführter Handlungen möglich und die Berechtigung an einer Transaktion gegeben ist.

6 INFORMATIONSSICHERHEITSPROZESS UND RISIKOMANAGEMENT

Der unternehmensweite Informationssicherheitsprozess stellt sicher, dass die Ziele und die Qualität des ISMS durch ein Modell mit den Phasen Plan, Do, Check und Act (PDCA-Modell gemäß ISO 9001) gewährleistet sind.

6.1 PLANEN DES ISMS (PLAN)

Das ISMS ist unter Federführung des ISB als PDCA-Modell geplant. Informations- und Sicherheitsobjekte sind unter Festlegung der Schutzwürdigkeit identifiziert und dokumentiert. Auf der Grundlage der Information Security Policy sind Sicherheitskonzepte und Richtlinien erstellt (wie z. B. Datensicherungskonzept, Virenschutzkonzept, Notfallvorsorgekonzept, Regelungen zur IT-Nutzung).

6.2 IMPLEMENTIEREN UND BETREIBEN DES ISMS (DO)

Die in der Planungsphase spezifizierten organisatorischen und technischen Regelungen und Maßnahmen sind implementiert und dokumentiert. Die aus dem operationellen Betrieb gewonnenen Ergebnisse sind als Protokolle oder andere Aufzeichnungen dokumentiert und stehen für Analysen zur Fehlerkorrektur und Verbesserung zur Verfügung.

6.3 ÜBERWACHEN DES ISMS (CHECK)

Alle Mitarbeiter sind verpflichtet, Sicherheitsvorfälle an ihren Vorgesetzten oder direkt an den ISB zu melden. Dies können z. B. Virenmeldungen, festgestellte Einbruchversuche, Verlust von mobilen Datenträgern, unzureichende Verfügbarkeit oder falsch dargestellte Informationen sein. Der ISB klassifiziert die gemeldeten Vorfälle und leitet die weiteren Maßnahmen ein. Die Wirksamkeit des ISMS wird jährlich durch den ISB im Rahmen interner Audits überprüft. Zusätzlich wird jährlich ein Audit durch die beauftragte externe Zertifizierungsstelle durchgeführt.

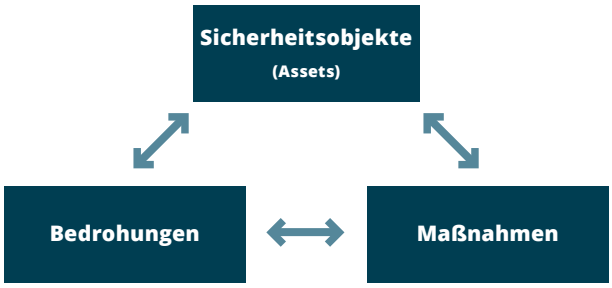
6.4 VERBESSERN DES ISMS (ACT)

Die bei internen oder externen Audits festgestellten Abweichungen und gegebenen Empfehlungen werden stets zeitnah geprüft und durch geeignete Maßnahmen umgesetzt. Die Wirksamkeit und Qualität des ISMS wird durch Kennzahlen bewertet.

6.5 RISIKOANALYSE

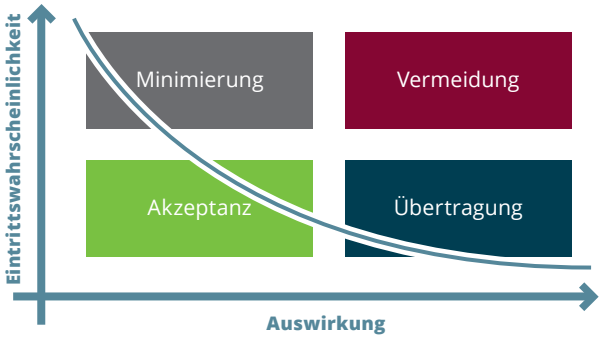
Risikoanalysen sind ein wesentliches Element des ISMS. Sie werden zur Identifikation und Bewertung von Risiken eingesetzt, um mögliche negative Ereignisse durch Präventionsmaßnahmen zu vermeiden, zu minimieren oder auf Dritte zu übertragen. Des Weiteren werden sie für die Kommunikation von Risikosituationen verwendet, um z. B. die Risikowahrnehmung zu fördern.

Ausgehend von den identifizierten Sicherheitsobjekten mit dem zugeordneten Schutzbedarf werden Szenarien betrachtet, aus denen potenzielle Bedrohungen der Schutzwürdigkeit erwachsen. Nach der Beurteilung der Eintrittswahrscheinlichkeit einer Bedrohung und der daraus resultierenden Schadenshöhe sind geeignete Maßnahmen technischer und organisatorischer Art zu ermitteln und bezüglich Implementierungsaufwand, notwendiger Realisierungszeit und Wirksamkeit zu bewerten.



Risikomanagement

In begründeten Fällen kann statt einer Vermeidung, Minimierung oder Übertragung von Risiken entschieden werden, ein Risiko aktiv zu tragen – soweit dies nicht gegen Gesetze, Vorschriften oder Verträge verstoßen würde. Eine solche Risikoakzeptanz ist immer der Entscheidung der Geschäftsleitung vorbehalten.



Risikobehandlung

7 SICHERHEITSVORGABEN UND STANDARDS

7.1 GESETZE, NORMEN UND STANDARDS

Die Einhaltung von Gesetzen, Normen, Vorschriften und Verträgen ist von höchster Priorität, wie z. B.:

- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
- BDSG (Bundesdatenschutzgesetz)
- TKG (Telekommunikationsgesetz)
- TMG (Telemediengesetz)
- ISO/IEC 27001

Die Aktualität der geltenden Gesetze, Normen und Vorschriften wird regelmäßig überprüft. Änderungen werden bewertet und fließen in die kontinuierliche Verbesserung des ISMS mit ein.

7.2 FLÄCHEN, GEBÄUDE UND EINRICHTUNGEN

Flächen, Gebäude und Einrichtungen, die von Mitarbeitern genutzt werden oder der Unterbringung von IT-Komponenten dienen, stellen den äußeren Schutz dar. Der Zutritt zu allen Flächen, Gebäuden und Räumen ist sicher geregelt und kontrolliert (Identifizierung, Einbruchschutz usw.). Flächen, Gebäude und Einrichtungen, die für Besucher und/oder Lieferanten zugänglich sind oder die Geschäftspartnern zur Verfügung stehen, sind durch geeignete technische und organisatorische Maßnahmen von den Teilen abgegrenzt, die ausschließlich von eigenen Mitarbeitern genutzt werden. In wichtigen Bereichen sind Gefahrenmelde- und Alarmsysteme installiert.

7.3 SERVER-RÄUME/BESONDERE FUNKTIONSBEREICHE

Der Zutritt zu Rechenzentren und zu anderen Räumen/Gebäudeteilen/Unterbringungen mit zentralen IT-Komponenten sowie zu Funktionsbereichen wie Personalwesen oder Geschäftsbuchhaltung ist nur dem hierfür autorisierten Personal gestattet. Diese Zutritte sind durch besonders wirkungsvolle Maßnahmen kontrolliert und geschützt.

7.4 INFORMATION RISK MANAGEMENT

Information Risk Management ist ein elementarer Bestandteil eines funktionierenden ISMS. Jeder Bereich der think project! Unternehmen überprüft seine Risiken und die dazugehörigen Maßnahmen regelmäßig auf ihre Wirksamkeit und Aktualität und passt diese an neue technische sowie andere Anforderungen an.

7.5 NEED TO KNOW

Der Zugriff auf die Betriebssysteme, Anwendungssoftware, Datenbanken/Dateien, Konfigurationsdaten usw. erfolgt nur durch speziell autorisierte Personen nach dem Need-to-know-Prinzip. Die Verfahren zur Systemadministration und Anwendung von IT-Komponenten sind bedarfs- und zielgruppenorientiert festgelegt.

7.6 UNTERBRECHUNGSFREIER BETRIEB

Bei Stromausfall stellt eine unterbrechungsfreie Stromversorgung den notwendigen Betrieb der wichtigsten Server, Netzkomponenten und Kommunikationseinrichtungen in ausreichendem Umfang sicher.

7.7 UMGEBUNGSBEDINGUNGEN

Soweit erforderlich verfügen IT-Räume über eine Klimaanlage zur Steuerung von Luftfeuchtigkeit und Temperatur. Sensible Komponenten (Disketten, Festplatten, Drucker, Scanner usw.) sind vor Verunreinigung (Staub, Verschmutzung) und vor starken Magnetfeldern geschützt.

7.8 DATENTRÄGER

Datenträger (Disketten, Magnetbänder, Removable-Disks usw.) für Sicherungen und Archivierungen lagern in feuerfesten Safes bzw. Räumen. Bei Bedarf sind diese „doppeltgetrennt“ gelagert.

7.9 VERKABELUNG

Die Verkabelung der aktiven und passiven Komponenten der Netze sowie der Endgeräte für Daten und Sprache ist in manipulationssicherer Form ausgeführt und die einschlägigen Vorschriften gemäß EMV/EMP sind erfüllt. Alle wichtigen Verbindungen sind sicher ausgelegt. Die Verkabelung ist vollständig dokumentiert und auch in gedruckter Form verfügbar. Unterbringungen mit Verkabelungskomponenten sind besonders gesichert und nur speziell autorisiertem Personal zugänglich.

7.10 WAN/LAN/WLAN

Das Netzwerk und seine Komponenten sind in wichtigen Abschnitten redundant ausgelegt und in gesicherten Räumen installiert.

7.11 EXTERNER ZUGANG

Der externe Zugang zu den Netzen/IT-Systemen für Fernwartungszugriffe und Extranet ist besonders geschützt. Der Zugang zu den angebotenen Internetdiensten ist durch geeignete technische Maßnahmen so abgesichert, dass nach Stand der Technik keine Manipulation dieser Dienste und keine Beeinflussung der internen IT-Systeme möglich sind.

7.12 INTERNETDIENSTE

Die Nutzung von Internetdiensten (Web, E-Mail, Instant Messaging usw.) erfolgt nach den betrieblichen Notwendigkeiten. Kriminelle, radikale, rassistische und pornografische Inhalte dürfen weder aufgerufen, erstellt noch gespeichert werden.

7.13 SOZIALE NETZWERKE/VIDEOPORTALE

Soziale Netzwerke werden ausschließlich nach unternehmensweiter Richtlinie in moderierter Form für Marketingzwecke sowie für die Kommunikation mit dem Nutzer als auch der Nutzer untereinander verwendet.

7.14 CLOUD-DIENSTE

Cloud-Dienste werden in mehreren Varianten verwendet. Bei der Auswahl und Überwachung der Cloud-Dienstleister werden die Bestimmungen zum Datenschutz eingehalten.

7.15 BRING YOUR OWN DEVICE

Den Mitarbeitern werden die notwendigen Geräte zur Erfüllung ihrer Aufgaben gestellt. Die Nutzung privat beschaffter Geräte zur persönlichen Arbeitsorganisation findet ausschließlich nach unternehmensweiten Richtlinien statt.

7.16 PC-ARBEITSPLÄTZE

Soweit erforderlich werden den Mitarbeitern geeignete elektronische Endgeräte bereitgestellt. Die Auswahl, Beschaffung und Konfiguration erfolgt zentral nach unternehmensweiten Richtlinien und entsprechend den funktionalen Erfordernissen. Abweichende Nutzung ist grundsätzlich untersagt und kann nur in Ausnahmefällen von der Geschäftsleitung genehmigt werden. Daten auf mobilen Endgeräten und mobilen Speichern ab der Vertraulichkeitsstufe „Confidential“ werden nach Stand der Technik verschlüsselt. Sicherheitsrelevante Updates werden bedarfsorientiert implementiert. Sicherheitseinstellungen dürfen von den Benutzern nicht deaktiviert oder verändert werden.

7.17 ZENTRALE DRUCKER

Gedruckte Unterlagen aus Druckern und Faxgeräten werden direkt nach dem Druck von dafür autorisiertem Personal entnommen.

7.18 VIRENSCHUTZ UND SCHUTZ VOR EINDRINGEN

Die Systeme und Netze sind durch geeignete technische und organisatorische Maßnahmen so geschützt, dass ein Befall durch Computerviren und ein Eindringen in diese Systeme nach Stand der Technik verhindert wird.

7.19 KONFIGURIERUNG

Konfigurationen werden nur von dem dafür autorisierten Personal vorgenommen und es sind Maßnahmen getroffen, die das Konfigurieren durch nicht autorisierte Personen verhindern.

7.20 ENTSORGUNG

Das Entsorgen von IT-Komponenten und die Vernichtung von Datenträgern (Papier usw.) erfolgt ausschließlich durch die hierfür zuständigen Stellen nach den Vorschriften der DIN 66399.

7.21 VERSCHLÜSSELUNG

Informationen in Abhängigkeit der Schutzstufen der Vertraulichkeit und Integrität werden bei der Speicherung und Übertragung durch geeignete Verfahren der Verschlüsselung gesichert.

7.22 DATENSICHERUNG/BACKUP/RESTORE

Datensicherungen werden regelmäßig durchgeführt. Die Lagerung der Datenträger dieser Sicherungen erfolgt in besonders geschützten Einrichtungen. Die Restore-Fähigkeit wird in regelmäßigen Abständen überprüft.

7.23 OUTSOURCING

Das Outsourcing von IT-Aufgaben und die Lieferung von IT-Komponenten sind – soweit sicherheitsrelevante Bereiche betroffen sind – besonders sorgfältig geplant und kontrolliert. Die entsprechenden Verträge berücksichtigen u. a.:

- Erfüllung von gesetzlichen Auflagen
- Vorgaben für die Kontrolle der Qualität des Outsourcing-Partners
- Durchführung von Kontrollmaßnahmen
- Notfallplanung bei Ausfall des Partners

7.24 NOTFALLPLANUNG

Für alle betriebsrelevanten Bereiche sind Notfallpläne erstellt. Diese Notfallpläne werden regelmäßig hinsichtlich ihrer Zielsetzung und Wirksamkeit unter Beachtung von Änderungen im Umfeld und der internen Gegebenheiten überprüft, angepasst und durchgeführt.

7.25 BUSINESS CONTINUITY

Der Aufbau eines leistungsfähigen Notfall- und Krisenmanagements zur systematischen Vorbereitung auf potenzielle Schadenereignisse, die wichtige Geschäftsprozesse gefährden, ist zwingend erforderlich.

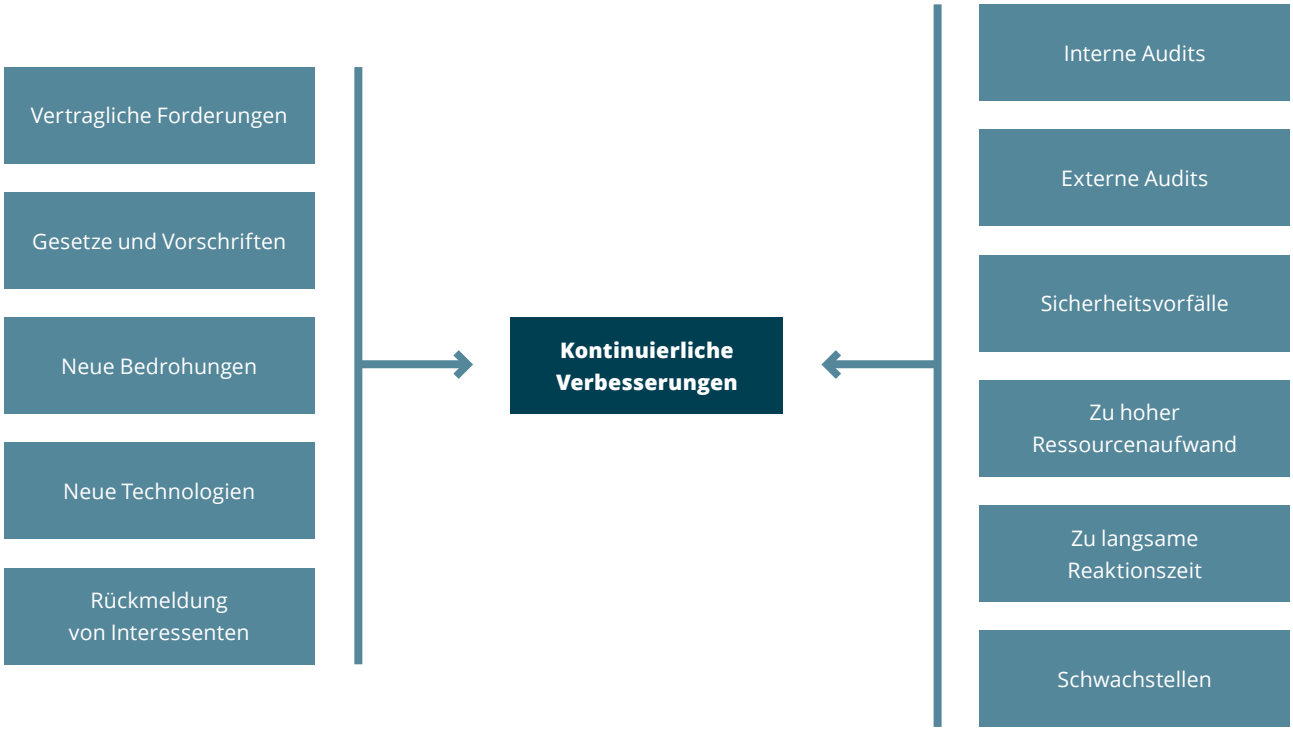
Dies betrifft nicht nur den IT-/System-Ausfall, sondern auch den

- Gebäudeausfall
- Ausfall von Personal
- Ausfall von Lieferanten/Partnern

Das Lebenszyklus-Modell zur Fortführung der Geschäftstätigkeit unter Krisenbedingungen oder zumindest erschwerten Bedingungen ist durch ein gestuftes Konzept von Maßnahmen abgesichert.

8 KONTINUIERLICHE VERBESSERUNG

Die Wirksamkeit des ISMS wird kontinuierlich verbessert. Korrektur- und Vorbeugungsmaßnahmen leiten sich aus unterschiedlichen Anlässen und Aspekten ab.



Auslösende Ursachen für kontinuierliche Verbesserungen

Die Schwerpunkte der kontinuierlichen Verbesserung liegen auf Vorbeugungsmaßnahmen und Maßnahmen mit der größten Wirkung bei möglichst geringem Ressourceneinsatz.

thinkproject!

50 Länder

10.000 Projekte

› 150.000 Nutzer

Über think project!

Weltweit sieht sich die Baubranche mit vielen Herausforderungen konfrontiert. Der Druck nimmt zu, Projekte innerhalb von Zeit- und Budgetgrenzen abzuschließen. Zudem muss eine stetig wachsende Menge an Daten bewältigt werden, die durch eine zunehmende Anzahl an Beteiligten in Bau- oder Ingenieurprojekten produziert wird.

Aus diesem Grund steigt der Bedarf für digitale Lösungen wie think project!, die sowohl die unternehmensübergreifende Zusammenarbeit als auch das Informationsmanagement vereinfachen.

Wir unterstützen unsere Kunden aus dem Bau- und Ingenieurwesen dabei, Digitalisierung zu verwirklichen, indem wir ihnen auf Basis unserer Branchenexpertise innovative Softwarelösungen sowie Beratung und Dienstleistungen zur Verfügung stellen.

think project! – Ihr Partner für den digitalen Wandel

Ansprechpartner weltweit
www.thinkproject.com/contact-us