[Logo der Organisation]

[Name der Organisation]

**PROJEKTPLAN**  
**für die Umsetzung des Informationssicherheits-Managementsystems**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Datum der Version: |  |
| Erstellt durch: |  |
| Genehmigt durch: |  |
| Vertraulichkeitsstufe: |  |

**Änderungs-Historie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Erstellt durch** | **Beschreibung der Änderung** |
|  | 0.1 | 27001Academy | Erster Entwurf des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Anwender 3](#_Toc36806391)

[2. Referenzdokumente 3](#_Toc36806392)

[3. ISMS Einführungsprojekt 3](#_Toc36806393)

[3.1. Ziel des Projekts 3](#_Toc36806394)

[3.2. Ergebnisse des Projekts 3](#_Toc36806395)

[3.3. Fristen 4](#_Toc36806396)

[3.4. Projekt-Organisation 5](#_Toc36806397)

[3.4.1. Projekt-Sponsor 5](#_Toc36806398)

[3.4.2. Projektmanager 5](#_Toc36806399)

[3.4.3. Projektteam 5](#_Toc36806400)

[3.5. Hauptrisiken im Projekt 6](#_Toc36806401)

[3.6. Werkzeuge für Projekt-Umsetzung, Berichtswesen 6](#_Toc36806402)

[4. Verwaltung von Aufzeichnungen zu diesem Dokument 6](#_Toc36806403)

[5. Gültigkeit und Dokumenten-Handhabung 6](#_Toc36806404)

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Projektplans ist die eindeutige Beschreibung der Zielsetzung für das Informationssicherheits-Managementsystem (ISMS) Einführungsprojekt, der benötigten Dokumente, der Fristen und der Rollen und Verantwortlichkeiten im Projekt.

Dieser Projektplan wird für alle Aktivitäten im Rahmen des ISMS Einrichtungsprojektes angewendet.

Anwender dieses Dokumentes sind Mitglieder des [Unternehmensleitung] und Mitglieder des Projekt-Teams.

# Referenzdokumente

* ISO/IEC 27001 Norm
* ISO 22301 Norm
* [Beschluss oder ähnliches Dokument in dem der Projektstart angeordnet wird]
* [Methodik für Projekt-Management]

# ISMS Einführungsprojekt

## Ziel des Projekts

Die Einführung des Informationssicherheits-Managementsystems gemäß der ISO 27001 Norm bis spätestens [Datum].

## Ergebnisse des Projekts

Im Verlauf des ISMS Einrichtungs-Projektes werden folgende Dokumente (einige davon enthalten Anhänge, die hier nicht ausdrücklich aufgelistet sind) erstellt:

* **Verfahren zur Lenkung von Dokumenten und Aufzeichnungen** – Regelwerk für die Erstellung, Genehmigung, Verteilung und Aktualisierung von Dokumenten und Aufzeichnungen
* **Verfahren zur Identifikation der Anforderungen** – Vorgehensweise für die Identifikation amtlicher, gesetzlicher, vertraglicher und anderer Verpflichtungen
* **Anwendungsbereich des Informationssicherheits-Managementsystems** – ein Dokument zur genauen Definition von Werten (Assets), Standorten, Technologien, etc. innerhalb des Anwendungsbereiches
* **Informationssicherheitspolitik** – ein zentrales Dokument für die Leitungs-Ebene zur Steuerung des Informationssicherheits-Managements
* **Methodik zur Risikoeinschätzung und Risikobehandlung** – Beschreibung der Methodik zum Umgang mit Informationsrisiken
* **Verzeichnis zur Risikoeinschätzung** – Ergebnis der Einschätzung von Werten, Bedrohungen und Schwachstellen
* **Verzeichnis zur Risikobehandlung** – Ein Verzeichnis in dem für jedes inakzeptable Risiko die entsprechenden Maßnahmen ausgewählt sind
* **Bericht Risikoeinschätzung und Risikobehandlung** – Dieses Dokument umfasst alle wichtigen Dokumente die während des Prozesses der Risikoeinschätzung und Risikobehandlung erstellt wurden
* **Erklärung zur Anwendbarkeit** – Ein Dokument das die Zielsetzung und Anwendbarkeit jeder Maßnahme nach Anhang A der ISO 27001 feststellt
* **Verfahren für interne Audits** – beschreibt wie Auditoren ausgewählt werden, wie Audit Programme erstellt werden, wie Audits durchgeführt werden und wie Audit-Ergebnisse protokolliert werden
* **Verfahren zu Korrektur** – beschreibt das Verfahren zur Umsetzung von Korrektur- und Vorbeugungs-Maßnahmen
* **Protokoll zur Managementbewertung** – ein Formblatt für die Protokollierung des Management-Meetings zur Bewertung der Angemessenheit des ISMS
* **Plan zur Risikobehandlung** – Umsetzungsdokument mit Beschreibung der umzusetzenden Maßnahmen, der Verantwortlichen für die Umsetzung, der Fristen und der Ressourcen

Weitere Dokumente die während der ISMS-Einrichtung erstellt werden müssen, sind im Plan zur Risikobehandlung spezifiziert.

Im Verlauf des Einführungsprojektes für betriebliches Kontinuitätsmanagement werden folgende Dokumente (einige davon enthalten Anhänge, die hier nicht ausdrücklich aufgelistet sind) erstellt:

* **Richtlinie für betriebliches Kontinuitätsmanagement** – Rahmenwerk für das BKMS zur Festlegung des Anwendungsbereiches und der Verantwortlichkeiten
* **Geschäftsauswirkungsanalyse (GAA) Fragebögen** – Analyse der qualitativen und quantitativen Auswirkungen auf das Geschäft, die notwendigen Ressourcen, etc.
* **Strategie für betriebliches Kontinuitätsmanagement** – Definiert geschäftskritische Aktivitäten, gegenseitige Abhängigkeiten, Zielsetzungen für Wiederherstellungzeiten, die Strategie für das Managen und die Sicherstellung des Geschäftsbetriebs, die Strategie zur Wiederherstellung von Ressourcen, die Strategien für einzelne geschäftskritische Aktivitäten
* **Plan für betriebliches Kontinuitätsmanagement** – eine detaillierte Beschreibung für den Umgang mit Katastrophen oder anderen Geschäftsunterbrechungen und für die Wiederaufnahme aller geschäftskritischer Aktivitäten
* **Plan für Training und Awareness** – eine detaillierte Übersicht, wie Mitarbeiter für die Ausführung geplanter Aufgaben geschult werden und wie deren Bewusstseinsbildung (Awareness) für die Wichtigkeit von Geschäftskontinuität umgesetzt wird
* **Übungs- und Test-Plan für betriebliches Kontinuitätsmanagement** – beschreibt wie Pläne geübt und getestet werden um notwendige Korrekturmaßnahmen zu identifizieren und den Plan zu verbessern
* **Plan zur Aufrechterhaltung und Überprüfung des BKMS** – eine detaillierte Übersicht die aufzeigt, wie Pläne und andere BKMS-Dokumente gepflegt werden sollten um deren Funktionsfähigkeit im Falle einer Geschäftsunterbrechung sicherzustellen
* **Formular zur Überprüfung nach einem Notfall** – ein Formblatt für die Überprüfung der Wirksamkeit von Plänen im Anschluss an einen Notfall
* **\***

## Fristen

Im Folgenden werden die Fristen für die Freigabe der einzelnen Dokumente im Verlauf der ISMS Einführung aufgeführt:

|  |  |
| --- | --- |
| ***Dokument*** | ***Fristen für Dokument-Freigabe*** |
| Verfahren zur Lenkung von Dokumenten und Aufzeichnungen | 30. Juni 20xx |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Im Folgenden werden die Fristen für die Freigabe der einzelnen Dokumente im Verlauf der BKMS Einführung aufgeführt:

|  |  |
| --- | --- |
| ***Dokument*** | ***Fristen für Dokument-Freigabe*** |
|  |  |
|  |  |
|  |  |
|  |  |

Abschließende Vorstellung der Projektergebnisse ist für den [Datum] geplant.

## Projekt-Organisation

### Projekt-Sponsor

Jedem Projekt ist ein „Sponsor“ zugeteilt, der nicht aktiv am Projekt teilnimmt. Der Projekt-Sponsor muss regelmäßig vom Projektmanager über den Projektstatus unterrichtet werden und greift ein, falls das Projekt unterbrochen wird.

[Name, Stellenbezeichnung] wurde zum Projekt-Sponsor ernannt.

### Projektmanager

Die Rolle des Projektmanagers umfasst folgende Aufgaben: Sicherstellung der für die Projekt-Umsetzung notwendigen Ressourcen, Koordination des Projekts, Information des Projekt-Sponsors über den Projektfortschritt, Durchführung von administrativen Aufgaben im Zusammenhang mit dem Projekt. Die Befugnisse des Projektmanagers sollten diesen in die Lage versetzen, die Projekt-Umsetzung ohne Unterbrechungen innerhalb der gesetzten Fristen sicherzustellen.

[Name, Stellenbezeichnung] wurde zum Projektmanager ernannt.

### Projektteam

Die Rolle des Projektteams umfasst folgende Aufgaben: Unterstützung bei verschiedensten Aspekten der Projekt-Umsetzung, Durchführung der im Projekt spezifizierten Aufgaben, sowie Entscheidungen zu verschiedenen Aspekten welche einen fachübergreifenden Ansatz erfordern. Das Projektteam kommt immer zusammen bevor die endgültige Version eines Dokumentes aus Abschnitt 2 dieses Projektplans erstellt wird. Außerdem in allen anderen Fällen für die es der Projektmanager als notwendig erachtet.

*Verzeichnis der Projekt-Teilnehmer*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Name* | *Organisationseinheit* | *Stellenbezeichnung* | *Telefon* | *E-Mail* |
| John Doe | IT department | System Admin | 00 1111-1234 | John.doe@yourcompany.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Hauptrisiken im Projekt

Folgendes sind die Hauptrisiken bei der Umsetzung des Projekts:

1. Überschreitung der Fristen in der Risikoeinschätzungs-Phase
2. Überschreitung der Fristen bei der Ausarbeitung der Pläne für Geschäftskontinuität
3. Durchführung von Aktivitäten, die unnötige Kosten und Zeitaufwände nach sich ziehen
4. Auswahl zu vieler und/oder zu kostspieliger Maßnahmen

Folgendes sind die Maßnahmen zur Reduzierung der oben genannten Risiken:

* Vom Projektmanager wird überwacht, dass alle Projekt-Aktivitäten zu den festgesetzten Fristen umgesetzt werden und er fordert vom Projekt-Sponsor zeitnah dessen Eingreifen an
* Es wird ein Berater engagiert um sicherzustellen, dass Zeiten und Ressourcen nicht auf für das Projekt unwichtige Aktivitäten verwendet werden und dass einzelne Aktivitäten nicht in die falsche Richtung gehen
* Es wird ein Berater engagiert der die effektivsten Maßnahmen empfehlen soll

## Werkzeuge für Projekt-Umsetzung, Berichtswesen

Auf dem lokalen Netzwerk wird ein gemeinsamer Ordner eingerichtet, der alle Dokumente enthält, die während des Projektes erstellt werden. Alle Mitglieder des Projektteams bekommen Zugang zu diesen Dokumenten. Nur der Projektmanager [und Mitglieder des Projektteams] werden die Berechtigungen dafür erhalten, Änderungen durchzuführen oder Dateien zu löschen.

Der Projektmanager wird einen monatlichen Projektumsetzungsbericht erstellen und ihn an den Projekt-Sponsor weiterleiten.

# Verwaltung von Aufzeichnungen zu diesem Dokument

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name der Aufzeichnung | Aufbewahrungs-Ort | Verantwortlicher für Aufbewahrung | Maßnahme zum Schutz der Aufzeichnung | Aufbewahrungs-Dauer |
| Projektumsetzungs-Bericht (in elektronischer Form) | Gemeinsamer Ordner für Projekt-bezogene Aktivitäten | Projektmanager | Nur der Projektmanager hat die Berechtigung, Daten zu bearbeiten | Der Bericht wird für die Dauer von 3 Jahren aufbewahrt |

# Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

Der Inhaber des Dokumentes ist [Stellenbezeichnung].

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

* Ob alle am Projekt beteiligten Mitarbeiter ihre Aktivitäten nach den Vorgaben dieses Dokumentes durchführen
* Ob alle Projekt-Fristen eingehalten werden

[Stellenbezeichnung]

[Name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Unterschrift]